Military and Strategic Affairs

Volume 6 | No. 2 | August 2014

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

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

Military and Strategic Affairs

Volume 6 | No. 2 | **August 2014**

CONTENTS

Military and Strategic Affairs

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

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

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

Editor in Chief: Amos Yadlin
Editor: Gabi Siboni
Editorial Board: Udi Dekel, Oded Eran, Zaki Shalom
Journal Coordinator: Daniel Cohen

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)

UN Peacekeeping Forces: Preventive Diplomacy and Its Limitations

Avi Beker

Despite UN peacekeeping forces' extensive activity in several conflict areas around the world, its abilities and effectiveness are limited. Furthermore, there is a lack of agreement and clarity regarding its legal and political aspects. The Israeli-Arab conflict has been the primary testing grounds in terms of developing the notion of peacekeeping during the Cold War, and stationing forces along and beyond Israel's borders has served as means of "preventive diplomacy." The end of the Cold War provided impetus for a number of peacekeeping initiatives and programs, though when faced with political realism and violent conflicts they did not prevail. Attempts to transform the troops into an intervening mechanism and type of defensive shield, using UAVs and other new technologies, are limited and indicative of the lack of agreement over the nature of the world order and the meaning of the collective security notion.

Keywords: UN peacekeeping forces, Security Council, responsibility to protect, UAV, Dag Hammarskjöld, Boutros Boutros-Ghali, Kofi Annan, Vladimir Putin, UNIFIL, UNDOF, UNEP

It is an interesting and even paradoxical fact that the largest, most intensive and most expensive United Nations' operation is rather an innovative practice which has no legal reference in the Charter of the organization.

According to UN data from May 2014, approximately 120,000 soldiers and administrators serve in UN forces worldwide, deployed in 17 different conflict zones involving over 100 nations, operating at an annual budget

Dr. Avi Beker is a lecturer in the Master's program in Diplomacy at Tel Aviv University and teaches International Law at the Ono Academic College. In the past he was a member of the Israeli Permanent Mission to the United Nations and served as the Secretary General of the World Jewish Congress.

of close to $8 billion. Since 1948, these forces have operated in 69 arenas worldwide – 54 of them since 1988 alone. The total number of casualties for those serving under the UN flag has already passed 3,200, even though the forces are not defined as combat troops.[1]

The only UN forces mentioned in the UN Charter are troops designated to operate against aggressive nations and elements posing a threat to peace, operating as part of the collective security mechanism mentioned in Chapter 7. By contrast, peacekeeping forces do not operate coercively; they operate on the basis of a mutual agreement between the sides involved in the conflict. The end of the Cold War and the fall of the Soviet Union inspired hopes of UN military troops' extensive involvement in conflict resolution. UN Secretary General Boutros Boutros-Ghali wrote a document which was presented to the Security Council in June 1992, in which he recommended establishing an army that would be under UN command and ensure international peace and security.[2] Ghali's idea of a force constructed of soldiers from UN member nations operating under the authority of the Security Council and command of the organization's Secretary General was well-received, garnering praise in editorials of leading newspapers, such as *The New York Times*, which called the new creation the "new world cops."[3]

22 years later, one cannot deny feelings of disillusionment. The notion that an international coalition would form to advance the idea of international intervention under the caption of a new norm of "responsibility to protect" was unrealistic.* The civil war in Syria, which to date has cost over 150,000 lives, turned approximately 2.5 million people into refugees and forced another 9 million people into internal exile from their homes (July 2014 estimates), is an excellent demonstration of the futility of both of the UN collective security system's roles: humanitarian intervention and the traditional practice of peacekeeping. The ability to intervene was taken off the table the moment that the politics of the Security Council brought about a face-to-face confrontation between its permanent members, as Russia and China cast a veto against any attempt at diplomatic condemnation of the atrocities perpetrated by Bashar Assad's regime. US Ambassador to the UN Susan Rice used the sharpest diplomatic language in criticizing the "disgusting" behavior of the two "intransigent" nations, saying the Security Council was being "held hostage" by them.[4] The status of the UN

* The notion became very popular in the literature of humanitarian intervention, earning its own acronym – R2P ("responsibility to protect") – in various written material.

forces in the Golan Heights buffer zone was undermined as troops were caught in the crossfire on the Syrian side. At the beginning of June 2013, the Austrian government announced the withdrawal of its troops from the Golan, close to four decades after the establishment of UNDOF (UN Disengagement and Observer Force).

The Middle East as Testing Ground

It is interesting to note that the Israeli-Arab conflict, in which the UN has achieved little success in peace making, had served as a main arena for the development of UN peacekeeping forces. In fact, the UN observers in 1948 and the disengagement force in 1957 provided the inspiration for the peacekeeping forces. In the Middle East, as in the other world conflict zones, UN forces attempt "preventive diplomacy," a notion that has no independent existence but can be an addition to ceasefire agreements, building on the interest shared by both sides not to resume the fighting. In 1948, UN observers were sent to the region to supervise the implementation of the armistice between Israel and its neighbors; following the October 1956 Suez crisis, UN forces were stationed in the Sinai Peninsula in 1957 whereupon the phrase "peacekeeping" was coined.

From the outset, it was clear that UN peacekeeping forces were an "improvisation" intended to overcome the paralysis plaguing the collective security system, preventing it from operating as envisioned by its founding fathers. Chapter 7 of the UN Charter refers to means of enforcement: "action with respect to threats to the peace, breaches of the peace, and acts of aggression," representing the heart of the collective security system that depends on cooperation among the permanent members of the Security Council-the five nations granted veto power. Chapter 7 states that, when diplomacy fails to resolve a conflict according to the means delineated in Chapter 6, the Security Council can implement diplomatic and economic sanctions against the "rogue state." Should these fail, the sanctions may be increased and augmented by a variety of military means, including permanent presence in the air, on land and at sea, under the authority of the Security Council. In the extremely fraught atmosphere of political and ideological conflict during the Cold War, and in light of the military rivalry and the nuclear arms race, the UN system of enforcement was doomed to recurring failure.

This deadlock created the need to circumvent the Charter's directives. Trygve Lie, the first UN Secretary General, initiated the establishment of UNTSO – the UN Truce Supervision Organization, the first UN observer force. The force was given the task of overseeing the armistice agreements' implementation along Israel's borders with its Arab neighbors. As Trygve Lie put it: "a small protective force essentially different from an attacking force."[5] UNTSO soldiers were often referred to, not without ridicule, as "soldiers armed with binoculars," though they rapidly became a permanent fixture of the Israeli-Arab conflict. To this day, they remain a constant mechanism charged with overseeing the implementation of agreements on the borders and assisting UN troops stationed in the region.

However, the essential breakthrough occurred when UNEF1 – the UN Emergency Force 1 – was established following the failure of the 1949 ceasefire agreement between Israel and Egypt and the 1956 Suez crisis, when it seized control of the Suez Canal along with British and French forces. Initiated by Canadian Foreign Minister Lester Pearson and UN Secretary General Dag Hammarskjöld, the formula for the peacekeeping force was born. Hammarskjöld viewed the force as a vehicle of "preventive diplomacy" whose scope slightly exceeds the directives of Chapter 6, which deals with the peaceful settlement of disputes while avoiding taking extreme enforcement steps such as sanctions and the use of military force discussed in Chapter 7. Expressing the improvisational nature of the peacekeeping force, which has no actual reference in the UN Charter, Hammarskjöld called it the directives of "chapter six and a half."[6]

In practice, UNEF1 was a peacekeeping force in military garb, including homogeneous battalions of regular soldiers from different countries stationed in the agreed-upon buffer zone on the Egyptian side of the Israeli-Egyptian border. Its role was to maintain the separation of forces between the respective armies and provide a mechanism of impartial supervision of the agreements' implementation in regards to the ceasefire and freedom of shipping from the Straits of Tiran to the Red Sea. UNEF1 then became the model for all subsequent UN peacekeeping forces, providing the formula described by Hammarskjöld as a "paramilitary force without military goals."[7] This was also the birthplace of the peacekeeping modus operandi-stationing forces only with the agreement of the parties involved, adopting an objective and impartial approach, limiting the use of force to self-defense, and the involvement of volunteer nations' troops with the exception of the five permanent members of the Security Council.[8]

Preventive Diplomacy?

UN officials do not hide their pride, boasting on the official UN website that the purpose of the peacekeeping force is to help "countries torn by conflict create conditions for lasting peace." The website further notes that UN forces "have built up a demonstrable record of success over our 60 years of existence, including winning the [1988] Nobel Peace Prize."[9] It would be somewhat pretentious to say that a ceasefire that generates an end to hostile activity without dealing with the root cause of the conflict can create true peace. Thus, in recent years, as part of the general trend of adopting openness and public penitence, the UN too had admitted the ineffectiveness of its peacekeeping force and, on several occasions, noted that its prestige has suffered because its "previous successes" have "raised expectations... beyond its capacity to deliver." The frustration, as explained by the UN, is the result of its involvement in conflicts during the 1990s in which "the Security Council was not able to authorize sufficiently robust mandates or provide adequate resources." The UN website refers directly to the conflicts in Yugoslavia, Rwanda and Somalia in which "the guns had not yet fallen silent" or "where there was no peace to keep." The UN points the finger at "warring parties [that] failed to adhere to peace agreements," and notes the peacekeepers' lack of resources and political support required to complete their mission.[10]

From the outset, it was clear that UN forces not operating on the basis of Charter arrangements for collective security would be unable to enforce peace. This was decisively proven by the very first peacekeeping force's task when UN Secretary General U Thant, Hammarskjöld's successor, responded to the demand by Egyptian President Jamal Abdul Nasser and, in May 1967, withdrew UNEF1 from the Israeli-Egyptian border without even bringing the issue to discussion before the Security Council, as required by the UN Charter itself. The hasty departure from the Sinai Peninsula was a significant factor in the deterioration of the crisis that led to the Six-Day War; Israel's fears and distrust of the UN were thus reinforced. As Foreign Minister Abba Eban so eloquently put it at the time: "It seemed as though the umbrella had disappeared just when it was starting to rain."[11]

The Responsibility to Protect

Towards the end of the Cold War, there was a sharp increase in the UN peacekeeping force's activities. Under US leadership, the only superpower left standing, an agreement was reached allowing the Security Council to authorize the establishment of 20 new task forces between 1989 and 1994, and increase the number of soldiers from 11,000 to 75,000. Some of the new missions in the early 1990s went beyond the traditional scope, expressing the directive of enforcement and the use of force. Troops were also stationed without the agreement of parties involved in the conflict. In some cases, the missions were very ambitiously defined, such as disarming militias (Somalia), enforcing the end of the conflict (in Bosnia, in conjunctions with NATO forces), and assuming all the powers of a temporary government on the road to creating a democratic regime (Cambodia).

Some of the objectives turned out to be impossible to attain. Furthermore, the UN demonstrated ineffectiveness in cases of abuse and genocide (especially in 1994, in Rwanda). This created an atmosphere of extreme frustration and accusations that resulted in a drastic drop in the deployment of peacekeeping forces in the second half of the 1990s. But after a short period of recovery, the number of forces continued to increase and hit new records in terms of manpower and budget. While the number of missions dropped, the number of those serving in the forces grew to 120,000. In some cases, peacekeepers were exposed to horrid behavior towards the local population, such as ignoring violations of human rights and even genocide, and stood accused of abuse, rape and human trafficking. All this forced the UN secretariat to establish a commission of inquiry, and several unflattering reports were issued, leading to stricter adherence to protocol. In most cases, the wrongdoing was not the fault of the peacekeepers alone, but rather the result of problematic direction and the lack of a clear interest on the part of the Security Council member nations.

The UN's failure to respond to humanitarian disasters and the appalling genocides in the 1990s paved the way to a new debate on the UN's role in peacekeeping and attempts to develop tools and goals that would meet the need for a more rapid and effective operative forces. At the beginning of the 21st century, the UN issued a long series of reports, three of which stood out in particular. These were put together by teams composed of many former statesmen and experts who recommended reforms in the UN system of collective security and peacekeeping.

The first of these reports (August 2000), written by the UN team for peaceful activities, is known as the Brahimi Report (named after Lakhdar Brahimi, the former Algerian Minister of Foreign Affairs and Under-Secretary of the UN, as well as, most recently, the UN Secretary General's delegate to Syria until May 2014). It listed the flaws of the existing structure and called to significantly strengthen the military force, along with more realistic directives for operating the troops. While the report accepted the peacekeeping forces' traditional rules of conduct, mainly serving as a buffer between armies, it also stressed the need to recruit forces that could respond to intra-state conflicts in which "one side to the peace agreement systematically and clearly violates its obligations." The report recognized the flaws and errors of the past and admitted that "the failure to distinguish between aggressor and victim" resulted in severe damage to "the UN status and credibility vis-à-vis its mission to keep the peace during the 1990s."[12]

The second report was issued in 2001 by the International Commission on Intervention and State Sovereignty (ICISS), which was established and funded by the Canadian government in conjunction with the UN, in order to develop a response to the challenge posed by UN Secretary General Kofi Annan: "If humanitarian intervention is, in fact, a violation of sovereignty, how can we respond to Rwanda, Srebrenica – severe and systematic violations of human rights that affect the image of humanity?" The commission developed guidelines for intervention by "the broader community of nations" in crises in which it is clear that sovereign nations "refused to or were incapable of" protecting their citizens against "disasters that could have been averted." Theoretically, one can say that this highly regarded team of statesmen and experts rejected the notion of the undisputed supremacy of sovereignty by saying that when a state fails to protect its citizens, it is the international community's prerogative to step in and use means of enforcement, including force, when necessary.[13]

In 2004, another prominent UN committee named "the global team for discussing threats, challenges and change in global security" discussed possible Security Council reforms, including the peacekeeping force. Though its report noted the new challenges, it failed to delineate any action points, limiting its recommendations to the establishment of another entity: the Peacebuilding Commission.[14] The report reaffirmed the notion of "responsibility to protect" raised in the ICISS discussions in 2001, defining it as "the new norm of collective responsibility to protect." It stressed the idea that when sovereign governments "cannot or will not" protect, it is the international community's obligation to intervene. This norm immediately received the UN Secretary General's approval and was later included in the General Assembly's resolutions (Resolution 1674). In 2009, despite the bitter failures in intervention and peacekeeping missions, UN Secretary General Ban Ki-Moon continued his predecessors' efforts and issued his own report regarding the responsibility to protect.

Confusion and Contradictions

It is hard to object to the esteemed value of "responsibility to protect," though experts on international law have questioned its validity from the outset.[15] During 2013, even its most ardent supporters discovered that the international community had adopted a very selective approach to implementing the concept. Critics accused the UN and its peacekeeping force of being "in league with evil," and claimed that "despite the Brahimi report and the [norm of] responsibility to protect, very little has changed in practice." UN forces, as well as UN member nations, "have not understood, nor have they internalized the meaning of invading another nation and assuming responsibility for doing so."[16]

While experts and statesmen in the UN and elsewhere continued to pride themselves on the new international relations' norm, a shocking humanitarian disaster had fallen upon Sudan, Darfur. After a period of hesitation, US Secretary of State Colin Powell joined the critics and called attention to the horrors, accusing the regime in Sudan of committing genocide.[17] In response to the international community's failure to intervene in Sudan, human rights' experts, such as Samantha Power (who became the US ambassador to the UN) and Morton Abramowitz wrote in 2004 that the UN had become a "broken system." According to Power and Abramowitz, the UN member nations were engaged in a hypocritical and cynical game, as they understood all too well that the Security Council would not rush to act. By shifting responsibility for the disasters of the world over to UN institutions, they were "passing themselves off as good world citizens." Power and Abramowitz summed it up as follows: "Major and minor powers alike are committed only to stopping those killings that harm their national interests. Why take political, financial and potential military risks when there is no strategic or domestic cost to remaining on the sidelines?"[18]

As long as the idea of intervention operates inequitably, it cannot be viewed as a legal norm possessing legal status. Why did the UN intervene in Somalia but not in Sudan? Why did UN and NATO forces operate in Yugoslavia but not in Chechnya? Why did the Security Council allow Libya to be bombed but didn't even allow a condemnation of the massacres in Syria? The selective approach is also evident in the total disregard of humanitarian law violations by Hizbolla, as by force of the directives of the UNIFIL (United Nations Interim Force in Lebanon) mandate and Resolution 1701 of August 2006, it is prohibited from arming since it is not part of the regular Lebanese military.

Stationing UAVs for Peacekeeping Purposes

At the beginning of July 2014, *The New York Times* published a report on the introduction of a new technological element into the UN peacekeeping force ranks: the UAV* (Unmanned – or Uninhabited – Aerial Vehicle). UAVs, used extensively by Israel, the United States and other nations, were stationed and operated by UN forces with the agreement of the Congolese government in other to gather intelligence about the rebels in Congo. The UN also received permission from Mali and the Central African Republic to operate UAVs in their territories where UN peacekeepers are already in place. South Sudan, where a UN force is also stationed, refused the UN's request to launch UAVs from its territory. In Congo, the UN operates UAVs only within the country's borders; it cannot investigate how arms are crossing into the country or if soldiers from neighboring Rwanda and Uganda are coming in, as these countries have refused introduction of UAVs into their airspace.[19]

Since 2008, and with greater impetus since early 2013, UN representatives and peacekeeping officers began speaking of the right to use UAVs as part of the UN forces' policing efforts. It seems that the United States, too, pushed for the introduction of UAVs into the UN's operational service, in part perhaps because of the growing criticism of the United States' use of weaponized drones for targeted killings (in Pakistan, Afghanistan and Yemen). As the talks began, human rights' organizations along with African and other nations expressed their reservations. Many relate to the concept with suspicion and hostility, as it seems like a cover for aggression and espionage on the part of the large, technology-rich (aka Western) powers.

* From the UN's perspective, the emphasis is on UAVs rather than drones or even Micro UAVs because the UN, for obvious diplomatic reasons, takes care to note that these are aerial vehicles without either pilots or weapons – nothing but flying cameras. Five Pelican model UAVs, made by Selex ES, belonging to Finmeccanica, an Italian conglomerate, were stationed in Congo. The cost of the UAVs was estimated at $15 million, a relatively small fraction of the force's annual budget of $1.45 billion.

From Israel's point of view, it is interesting to note that in a Security Council debate in June 2013, the UNIFIL forces' commander Paolo Serra (Italy) expressed the need to bring similar technology to the Israeli-Lebanese border, so that his soldiers could more effectively supervise the so-called blue line (the international line between Israel and Lebanon).[20] As noted, despite the prohibition explicitly delineated in Resolution 1701 on moving arms to Lebanese militias that are not part of the Lebanese army, UNIFIL refrained from reporting transfers of arms from Syria to Hezbollah. According to standard practice, as demonstrated above, nations need to agree to the stationing of UN forces on their territory, but one cannot rule out the possibility that, in the future, demands will be made of Israel to allow UAVs in its territorial skies for supervising both sides of the Israeli-Lebanese border, other borders, and even as part of security arrangements along the Jordan Valley. As past experience has shown, even if the UN is incapable of enforcing security arrangements on Israel (as long as the United States has veto power) it can serve as a diplomatic tool for international pressures wielded by whoever steers the will of the majority of the General Assembly.

Intervention Force: The Exception

There is disagreement among scholars and politicians about UN peacekeeping force's contribution and necessity. From time to time, the topic is raised in the US Congress, which funds about one-fourth of the peacekeepers' budget (completely separate from the UN budget).[21] One can certainly point to the UN's selective approach to peacekeeping missions based on global politics and the different characteristics of areas of conflict. While the UN had failed to intervene in the case of the Syrian massacres, it was able to strengthen its forces in Congo under a mandate formulated in the spirit of "responsibility to protect." In March 2013, the Security Council renewed the peacekeeping force's mandate in the Democratic Republic of Congo and, for the first time, provided the authority to use offensive military force. According to the Secretary General's recommendations and in response to the call of 11 African states from the Great Lakes region, the Security Council unanimously decided (in Resolution 2098) to operate "a military intervention brigade" that would act as part of a force of almost 20,000 stationed in the region. According to the resolution, the brigade has the authority to embark on an offensive mission – whether initiated or as a response – together with or apart from Congolese army forces "while defending itself, and maintaining high levels of mobility and flexibility" in order to achieve "paralysis and disarmament" of the insurgents and foreign forces in Congo.

In the past, the UN Security Council used formulations that referenced Chapter 7 against world peace violators, such as the First Gulf War in 1991 (against the Iraqi invasion of Kuwait led by Saddam Hussein) or the war in Afghanistan after the 9/11 terrorist attacks. However, in those cases it would be more accurate to say that the Security Council had delegated its authority to the United States, as it led the coalition of states that were willing to use "all the necessary means" to restore peace. In the case of Congo, it was the resolute will of the nations in the region to bring some relief to the horrific, ongoing war of many years – also known as the Great African War – that has killed and maimed millions. In the debate, Russia and China, which usually refuse to approve international community interventions, stressed that the mandate approval is not a precedent, but rather "a unique and exceptional case."[22]

The peacekeeping force in Congo and the mandate given to the French intervention force in Mali by Resolution 2085 (January 2013) are the exceptions to the rule, proving that there has been no fundamental change in the large powers and UN approach to the notion of "responsibility to protect." These are events taking place in the heart of the African continent in which nations are trying to confront internal and external subversion. China and Russia, the most adamant opponents to intervention in sovereign nations' internal affairs, were forced to concede for fear of angering the African nations that represent the largest bloc of nations in the UN. For African countries, it is important to promote the initiative to fight the insurgents and mercenaries in the war-torn continent that is riddled with enemy tribes and failed states. Unlike Africa, the events in Syria demonstrate the extent to which peacekeeping forces revert to Cold War patterns of conduct; they are only capable of functioning as means of preventive diplomacy in buffer zones on condition of the involved parties' agreement and at the behest of the large powers, and cannot touch upon the roots of the conflict.

Furthermore, crises involving obvious large power interests, humanitarian intervention and the notion of responsibility to protect are doomed to failure. Russia's opposition on June 8, 2013, to the UN attempt to declare Syria a no-fly zone was fervent and explicit. Russian Foreign Minister Sergei Lavrov warned the world against "a violation of international law," thereby voicing

Russia's anger about the previous Security Council decision in which the peacekeeping notion and the principles of "responsibility to protect" were implemented by means of a no-fly zone over Libya, becoming the basis for bombing the state and collapsing the Gaddafi regime.

Moreover, it is clear that Russia wishes to revisit the principles upon which the peacekeeping forces were established almost 60 years go. On June 13, 2013, Russian President Vladimir Putin proposed that Russian forces replace the Austrian force that had announced its withdrawal from the Golan Heights. After the UN spokesperson announced that this contradicted the 1974 Israel-Syria separation of forces agreement, according to which forces belonging to the permanent members of the Security Council shall not join UNDOF, Russian Ambassador to the UN Vitaly Churkin responded by saying that "times have changed since the agreement was signed 39 years ago." According to the ambassador, UNDOF was in crisis and the Russian offer was intended to help.[23]

Non-UN Forces

In several cases, due to the UN's inherent hostility towards Israel, negotiations between Israel and its neighbors have given rise to the use of non-UN observer and buffer forces. For instance, the peace agreement between Israel and Egypt in 1979 was brokered by the US, facing vehement opposition in the Arab world as well as within the UN General Assembly and Security Council. Following the Soviet Union's threats in the UN Security Council to veto the stationing of a peace force in Sinai, as stipulated in the military addendum to the peace treaty, Israel, the US and Egypt initiated the establishment of a peacekeeping force that would operate outside the UN framework (an option already formulated in the treaty). The force was set up using the infrastructure established in the interim accords between Israel and Egypt, based on the American force that was stationed in Sinai in 1975 in order to oversee and coordinate the initial stages of the Sinai withdrawal.

Following the signing of the protocol on August 31, 1981, the Multinational Force and Observers (MFO) was established. It was deployed on April 25, 1982, upon the official completion of the Israeli withdrawal from Sinai. The MFO supervises the military arrangements between the parties according to the peace treaty, and conducts patrols and periodic inspections. The force is led by an American commander stationed in Rome and includes 1,600 soldiers of varying nationalities, mainly Western countries.[24]

Another international force was established following the February 1994 massacre in the Cave of the Patriarchs in Hebron, where an Israeli by the name of Baruch Goldstein killed Muslim worshippers. UN Security Council Resolution 904 was passed in March 1994, condemning the murder, and calling for the adoption of preventative measures, including, among other things, the presence of foreign observers in the city. This was the scope of the UN involvement, as it had no further connection to its deployment and operation. The team of observers was called the Temporary International Presence in Hebron (TIPH). It was established in an agreement between the Palestinian Authority and Israel, and began operating in May 1994. Its operations were discontinued in August 1994, and resumed in May 1996. The observers, led by the Norwegian government, patrol Hebron and provide information to the IDF and the Palestinian police force. TIPH's mandate is renewed by Israel and the Palestinians every six months. It appears that mutual diplomatic interest has helped both sides overcome several incidents such as the murder of two observers by an armed Palestinian in 2002, rioting by Palestinians, and isolated altercations with Jewish residents.[25]

The European Union Border Assistance Mission at the Rafah Crossing Point (EUBAM Rafah), launched as part of the European Union's security and defense policy on November 24, 2005 serves as yet another example of positive international intervention via preventive diplomacy. According to its official website, EUBAM's activity was suspended in June 2007, following "the Hamas takeover of the Gaza Strip."[26] The EU mentions its policy of no contact with Hamas, and notes that in accordance with the authorization obtained from its institutions, "We will remain in the region with an operational capability to deploy on short notice." The suspension of its activity in the field led to a significant reduction in the number of forces, leaving 18 international team members and eight local staff in regular contact with the parties, maintaining a basis for the force's return "on short notice."

During the humanitarian ceasefire in Operation Protective Edge, prior to any meaningful negotiations, European representatives have suggested resuming the task force's operations. On August 7, 2014, German, French and British ambassadors presented their proposal for the Gaza Strip reconstruction to the Israeli Ministry of Foreign Affairs, subject to a supervisory mechanism that will prevent Hamas from rearming. The proposal included an international mechanism that would prevent the entry of forbidden materials to the Gaza Strip, verifying that double-use materials, such as cement and iron, would not reach the hands of terrorist organizations. The representatives mentioned the possibility of reactivating EUBAM at the Rafah Crossing, alongside Palestinian Presidential Guard forces.[27]

It is too early to examine any long-term ceasefire agreement and its derivatives, though if a ceasefire agreement is formed it will inevitably revive the new-old diplomatic mechanism of supervised border crossings. Diplomacy, which is sometimes also called "the art of the impossible," frequently succeeds in creating formulas and tools, even when it is clear to the parties involved that it cannot provide security, or even any degree of basic trust between the parties to a conflict. Even when the UN is unable to take part in an arrangement, as had happened in Sinai, Hebron, and the Gaza Strip, creative ideas for an international involvement are possible. At the same time, experience proves that just as UN forces are incapable of providing the means for enforcing peace, non-UN buffer and supervision may not be a reliable mechanism for deterrence and preventing security escalation.

Peacekeeping Smoke Detectors

It seems that instead of being a means of enforcement in the spirit of collective security as mentioned in the UN Charter, the debate about the peacekeeping force increasingly reflects disagreements among the powers regarding the manner in which world order should be preserved. Security Council resolutions regarding central Africa indicate the very limited and selective implementation of the idea of intervention by means of UN forces. Debates in the UN reflect the fact that Russia and China are reluctant to increase the forces' involvement. Nevertheless, they accept some limited compromises in order to avoid conflict with the coalition of African states that view the UN as means for maintaining stability and order an area riddled with revolt and subversion.

The experience accumulated in the course of the Israeli-Arab conflict indicates that peacekeeping forces are only effective when they are stationed as part of an agreement that exceeds the mere cessation of violence, even if only temporary. Such agreements, involving the Security Council as well, include other diplomatic and security measures that are used to maintain a deterrent force. At times, when the UN peacekeepers are joined by other elements, they may be construed as trust building measures. In the reality of the Middle East, their presence affords a psychological element of stability.

Attempts to convert the idea of peacekeeping to "responsibility to protect" and a mechanism of intervention have proven to be unrealistic and reveal, yet again, the ineffectiveness of measures dependent on some vague reference to "chapter six and a half" of the UN Charter. The lack of legal clarity and political initiative cast another shadow on the credibility of peacekeeping forces as means of preventive diplomacy. Alongside some partial success stories, there is the risk that, in times of crisis, the UN peacekeeping force may fail even at the smallest attempt at issuing a warning about impending deterioration. Just as diplomacy does not always succeed in preventing crises and outbreaks of violence, so is a UN force liable to serve as a smoke detector only after a fire has already erupted.

Notes

[1] From the UN official website, http://www.un.org/en/peacekeeping/resources/statistics/factsheet.shtml.

[2] Boutros Boutros-Ghali, "Empowering the United Nations," *Foreign Affairs*, Winter 1992-1993.

[3] "The New World Cops," *New York Times*, June 28, 1992.

[4] Explanation of Vote by Ambassador Susan E. Rice, US Permanent Representative to the United Nations, at a Security Council Session on Syria, February 4, 2012, http://usun.state.gov/briefing/statements/183334.htm.

[5] "Trygve Lie, 1946-1953," in *Public Papers of the Secretaries-General of the United Nations*, ed. Andrew W. Cordiers and Vilder Foote (New York: Columbia University Press, 1969), p.131. For more on collective security and the activities of the peacekeeping force: Avi Beker, "Peacekeeping and Peace-unmaking," in *The United Nations and Israel: From Recognition to Reprehension* (Massachusetts: Lexington Books, 1988), and Avi Beker, "The United Nations and Security Regimes: The Unfulfilled Vision" in *Security Regimes in the Middle East*, ed. Efraim Inbar (New York: State University of New York Press, 1995).

[6] A. Leroy Bennet, *International Organizations* (Englewood Cliffs, N.J.: Prentice-Hl, 1980), p.1980 and in http://www.unis.unvienna.org/unis/en/60yearsPK/index.html.

[7] Introduction to the Annual Report of the Secretary General on the Work of the Organization, June 16, 1959-June 15, 1960 *General Assembly Official Records*, 15th session Supplement No. 1A, (A/4390/Add.1).

[8] As formulated by the former UN Under-Secretary General for Political Affairs Sir Brian Urquart, *A Life in Peace and War* (New York: Harper and Row, 1987), p. 198.

[9] "History of peacekeeping," UN, https://www.un.org/en/peacekeeping/operations/peacekeeping.shtml.

[10] "History of peacekeeping," UN, https://www.un.org/en/peacekeeping/operations/surge.shtml.

[11] John G. Stoessinger, *The United Nations and the Superpowers* (New York: Random, 1977), p. 100.

[12] *The Panel on United Nations Peace Operations*, August 2000, chaired by Lakhdar Brahimi, former Minister for Foreign Affairs of Algeria and Under-Secretary General of the UN. In particular paras. 48-64; see http://www.un.org/peace/reports/peace_operations/.

[13] Evans, Gareth; Sahnoun, Mohamed, Co-chairs (2001). *The Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty*. Ottawa, ON, Canada: International Development Research Centre, Minister of Foreign Affairs.

[14] "A More Secure World: Our Shared Responsibility," Report of the High Level Panel on Threats, Challenges and Change of the United Nations, December 2004, http://www.un.org/secureworld/.

[15] Carsten Stahn, "Responsibility to Protect: Political Rhetoric or Emerging Legal Norm?" *American Journal of International Law* (2007): 99-120.

[16] Adam Lebor, "*Complicity with Evil" – The United Nations in the Age of Modern Genocide* (New Haven, Yale University Press, 2006), p. 275.

[17] Rebecca Hamilton, "Inside Colin Powell's Decision to Declare Genocide in Darfur," *The Atlantic*, August 17, 2011, http://www.theatlantic.com/international/archive/2011/08/inside-colin-powells-decision-to-declare-genocide-in-darfur/243560/, and see Adam Jones, *Genocide A Comprehensive introduction* (New York: Routledge, 2011) p. 373.

[18] Morton Abramowitz and Samantha Power, "A Broken System," *Washington Post*, September 13, 2004, http://www.washingtonpost.com/wp-dyn/articles/A17059-2004Sep12.html.

[19] "Unarmed Drones Aid UN Peacekeeping Missions in Africa," *New York Times*, July 3, 2014, http://www.nytimes.com/2014/07/03/world/africa/unarmed-drones-aid-un-peacekeepers-in-africa.html?_r=1.

[20] "Drones Bolster UN Peacekeeping Capabilities," *VOA News*, June 26, 2013, http://www.voanews.com/content/drones-un-congo/1690092.html. For more on the presentation of the UN's purpose in using UAVs:. "UN Forces Use Drones for First Time, in Eastern Congo" *Reuters* –Dec 3, 2013, http://www.reuters.com/article/2013/12/03/us-rop-congo-democratic-drones-idUSBRE9B20NP20131203.

[21] See two opposing views: Micah Zenko et al., "The Case for UN Peacekeeping Expert Brief," *Council on Foreign Relations*, March 2, 2011, http://www.cfr.org/peacekeeping/case-un-peacekeeping/p24277, and Brett Schaefer, "Critical Reforms Required for UN Peacekeeping," *The Heritage Foundation*, Sep 8, 2009, http://www.heritage.org/research/reports/2009/09/critical-reforms-required-for-un-peacekeeping.

[22] See the references to the "exceptional basis" of the mandate in the UN announcement: "'Intervention Brigade': Resolution 2098 (2013) Enables 'Offensive' Combat Force To 'Neutralize and Disarm' Congolese Rebels, Foreign Armed Groups," http://www.un.org/News/Press/docs/2013/sc10964.doc.htm, and background story: "Deployment of Intervention Brigade is Not Peacekeeping But Peace Enforcement," *The Guardian*, May 5, 2013, http://www.guardian.co.uk/world/2013/may/05/un-force-democratic-republic-congo.

[23] "Russia Offers Peacekeepers for Golan Heights, " *AP Report, ABC News*, June, 7 2013, http://abcnews.go.com/International/wireStory/russia-offers-peacekeepers-golan-heights-19348663 and, http://www.npr.org/blogs/thetwo-way/2013/06/15/191934306/russia-says-no-fly-zone-over-syria-would-be-illegal.

[24] "A New Reality on the Egypt-Gaza Border" *Policy Watch 518*, The Washington Institute, September 19, 2005, http://www.washingtoninstitute.org/templateC05.php?CID=2374.

[25] See TIPH website http://www.tiph.org/.

[26] See Hebrew version of the EUBAM website http://www.eubam-rafah.eu/he/content/%D7%A9%D7%90%D7%9C%D7%95%D7%AA-%D7%A0%D7%A4%D7%95%D7%A6%D7%95%D7%AA.

[27] "Europe: Gaza Restoration in Return for Supervising the Terror Organizations' Arming," *Haaretz*, August 7, 2014, http://www.haaretz.co.il/news/politics/.premium-1.2399479.

Changing Trends in Unmanned Aerial Vehicles: New Challenges for States, Armies and Security Industries

Liran Antebi

In recent years, the use of unmanned aerial vehicles has been on the rise. However, there is an evident change in constituent components. As the number of countries utilizing these vehicles continues to increase, the manufacturing process has been revolutionized, allowing many nations and commercial companies to manufacture and sell UAVs to the highest bidder. The changes in manufacturing processes have given rise to an expansion of their possible use, including terror. These changes require a reevaluation in order to face the dangers and enjoy the advantages created by them.

Keywords: UAVs, robots, states, aerial defense, terrorist organizations, military industries, technology

Introduction

The continuing increase in the use of Unmanned Aerial Vehicles (UAVs, also known as drones) is nothing new. Over the course of almost two decades, they have constituted a fascinating field in terms of technology, economy, and tactical and strategic impact. While the use of UAVs continues to grow, the factors influencing that use are changing, posing a significant challenge to international actors.

The current paper posits that the changes in trends regarding UAVs extend beyond the frequency of their use and acquisition in the military realm, as UAVs are entering the civilian and commercial spheres. Consequently, the paper examines these changes along with trends-within-the-trend

Liran Antebi is a Neubauer Research Fellow and head of Military Technology Research at the Institute for National Security Studies. She is also a PhD candidate in Political Science at Tel Aviv University.

at the state level, in the military, military industries and technological enterprises, seeing as the formulation of appropriate policies in the field and their correct implementation may generate many potential benefits.

It is the author's assertion that decision makers and the security establishment must pay attention to these changes, prepare for threats and exploit the opportunities stemming from technological developments in the UAV field.

Steady Growth in the Use of UAVs

Over the course of the past two decades, technological developments and the miniaturization of powerful computer capabilities have led to far-reaching changes in the machines surrounding us.

Consequently, the use of unmanned tools and robots has dramatically increased in diverse fields such as industry, transportation, medicine, household maintenance and security and military applications. A significant change took place when the United States engaged in offensive action in Afghanistan and later in Iraq, creating the need for military solutions, some of them in the form of unmanned vehicles, with an emphasis on the aerial dimension.

According to the US Department of Defense, "an unmanned platform" is "an air, land, surface, subsurface, or space platform that does not have the human operator physically onboard the platform."[1] There are currently many different types of aerial platforms used in the military, from miniature vehicles the size of a small bird or even an insect, through small and mid-sized vehicles that can be carried by a single soldier or small team and later assembled in the field, similar to or even larger than manned vehicles. These platforms differ from one another in their flight altitude, effective range, and most importantly the tasks and missions they are designed to carry out.

The United States was and remains (as of 2014) the leader in terms of UAV development, manufacture and use. In 2001, when US troops engaged in an offensive in Afghanistan, the United States operated some 60 UAVs. By 2012, the United States had more than 7,000 UAVs, representing about 31 percent of all aerial vehicles in the United States Armed Forces, including the small UAVs operated by ground forces.[2]

As a result of the growing operational use, there has been a significant increase in the budgets allocated by the US administration for UAV research and development, acquisition and training. In 2001-2013, the US administration allocated $26 billion to the field, a significant increase from the 1988-2000 budget of $3.9 billion.[3]

The United States is not the only country with a long record of developing, manufacturing and using UAVs: Great Britain, Germany, France, Israel, India, Turkey and Italy have also been involved in UAV development and manufacturing. The European nations, for instance, have accumulated operational experience in deploying these vehicles during the war in Afghanistan.

The systems' proliferation (mainly small UAVs) and the reduction of costs and obstacles to entering the field (such as the ability to make effective use of them) currently allow a more widespread use by private individuals, companies and countries with limited financial resources.[4] This constitutes a change from the past decade, in which UAVs were used for military purposes by an exclusive group of nations. Between 2005 and 2011, the technologies' reduced cost caused an increase in proliferation, as the number of countries operating UAVs grew from 40 to over 70. Some of these countries have the capability to independently develop and manufacture these vehicles.[5] Consequently, several trends have emerged in the field and shall be discussed in the following sections.

Factors Facilitating Change

Changing trends are often the result of certain factors and are facilitated by others. The following section will discuss the factors facilitating the changing trends in unmanned platforms.

a. **Rapid technological development:** over the course of the past decade, the rate of technological development has been accelerating in perhaps the fastest pace in human history. The current changes are based on a revolution in information technologies beginning in the 1980s. During the 1990s, information technologies ripened into the "information revolution," catalyzing extensive changes in various fields, including military doctrines of warfare.[6]

b. **Reduced cost:** improvements and advances in research and development lowered the costs of technologies. While some technologies remain very costly and relatively rare (e.g., supercomputers), what was once considered a "supercomputer" (for instance, during the "Space Race") is now at the fingertips of anyone with a smartphone.

c. **Globalization:** despite some limits, the impact of the global village often minimizes the geographical distance between individuals.

d. **Availability:** Technologies are becoming increasingly available not only because of their reduced cost but also because of the ability to trade and transport commodities, whether via the Internet or by other means. In other words, lowered costs along with globalization give rise to availability.

e. **Lack of legislation and regulation:** Technology is outpacing law, since the legislative and legal systems must become acquainted with technology and must engage in long bureaucratic processes in order to produce relevant legislation and enforcement. As a result of the incongruent development speed, technology with harmful potential may develop to the point of no return with neither local nor international legislation being able to limit its development or use.

New Manufacturing Actors

Another change is taking place among UAV manufacturers. In the past two decades, the two leaders in the manufacturing and sale of UAVs have been the United States and Israel. Both countries have large UAV industries and enjoy significant operational experience.[7] The United States is the leading country both in the development and manufacturing of UAVs and in their use around the world. Throughout the years the main designation for US-manufactured UAVs has been military, and currently the US armed forces are in control of a fleet of over 7,500 UAVs.[8]

Although it is a relatively small country, from 2005 until 2013 Israel was the world leader in UAV export.[9] According to various unofficial reports, Israel exported UAVs to almost 50 nations including Australia, Croatia, France, Germany, Singapore, Thailand, Turkey and the United States, and these are just the tip of the iceberg.[10]

Both the United States and Israel have introduced new models in the past year, such as the Israeli Super Heron and the US X-47B. These are generally large platforms and sometimes have advanced capabilities such as very long flight ranges, aerial attack capabilities, stealth capabilities and autonomous (i.e., requiring no human intervention) takeoff and landing capabilities. Nevertheless, as of the middle of 2012, almost 50 countries were manufacturing roughly 900 different types of UAVs.[11]

Europe

European nations, mainly Germany, Great Britain and France, have also been developing, manufacturing and selling UAVs, though their industry was not as developed or large as that of the United States and Israel. A prominent example is the unique joint effort between Britain and France announced in 2010[12] whose first product is a UAV called the nEUROn- a combat UAV with stealth capabilities.[13] Other countries involved in the project were Italy, Sweden, Switzerland, Greece and Spain. Similarly, Germany and Spain are working together to develop a combat UAV called the Barracuda, supporting capabilities that are similar to the nEUROn. These ambitious programs are evidence of a European attempt to collaborate in order to close the gap and enter the market currently controlled by the US and Israel.

Russia

The Russian leadership is well aware of the contribution of UAV technology to US military capabilities and operations, including the extension of its operations to regions in which it is not physically present at a fraction of the cost of military intervention and with little to no media attention. Along with economic factors, this served as an impetus for the Russian national program in the field of unmanned platform development. Russia intends to invest $9 billion by the year 2020 in a project to develop UAVs with intelligence gathering, communications and combat capabilities. These platforms are intended to join the fleet of some 500 UAVs, primarily manufactured by the United Arab Emirates and Israel.[14] The Russian initiative indicates a trend common to large, powerful nations seeking to control and assert their power in the international arena.

China

Another national program, perhaps even more worrisome to the west than the Russian one, was initiated in 2011 by the Chinese government. At the time, the Chinese regime announced its intention to match the United States' UAV fleet and even create a larger one.[15] The Chinese have articulated a plan of action and are working assiduously to realize it, the products of which are presented in various military parades.[16]

China is currently equipped with hundreds of UAVs, and in 2011, for instance, it operated 280 vehicles.[17] Furthermore, it is a member of the relatively exclusive group of nations manufacturing UAVs with attack capabilities. However, unlike other nations making such vehicles, China is not a signatory to treaties restricting their sale (such as the MTCR or WASSENAAR agreements). Consequently, these vehicles may find their way to various buyers, and may even undermine the familiar balance of power in the international arena. In addition, nations that for ideological reasons are opposed to purchasing technologies from the United States or Israel may use China to acquire such equipment. Moreover, according to several reports, Chinese hackers are busy breaking into and stealing US drone software and technology, which could enable China to utilize similar programs.[18] However, the Chinese conduct is not the only worrisome factor in this context. Another element liable to undermine the familiar balance of power is the entrance of small countries into the field of UAV manufacturing, which until now was reserved for nations with great industrial and military strength.

Small Nations

Technological changes may give rise to the introduction of small nations into the field. If, in the past, the privilege of utilizing unmanned capabilities (for operational military purposes rather than in amateur settings) was reserved for advanced nations with highly developed military industries – the superpowers and their allies – the current trends indicate a change, mainly due to the lowered cost of the technologies involved. However, such nations joined the group of states using UAVs already in the middle of the first decade of the 21st century. By the beginning of the second decade, another change had occurred: small nations began to develop and manufacture these vehicles themselves. The new phenomenon is also the result of lowered costs as well as globalization and the rapid and free transmission of information and data theft.

The trend is affecting each and every continent. Today, UAVs are manufactured virtually everywhere, including Ethiopia[19] and Nigeria[20] in Africa, who have both unveiled domestically produced unmanned platforms, along with Colombia[21] and Venezuela[22] in South America, in addition to North America, Europe, the Middle East and Asia.

One of the most intriguing countries riding the bandwagon is Iran. Iran is not considered a superpower, and in recent years it has been subject to economic and military sanctions. Nonetheless, on more than one occasion over the past few years it has unveiled domestically developed UAVs. Iran is developing – individually, or with, for example, Venezuela – several types of unmanned platforms, including those with combat and even stealth capabilities. If indeed its statements are true, Iran would be the most prominent demonstration of the change in the field: the economic embargo placed on Iran, previously preventing it from acquiring platforms such as UAVs, can no longer prevent the attainment of such technology, even combat UAVs with a flight range of 2,000 kilometers.[23] Domestic scientific and technological capabilities, global changes, and possibly the use of stolen technologies have allowed Iran to circumvent the international sanctions. The new vehicles are essentially different from the first Iranian UAV called the Ababil, a relatively simple explosive UAV put into service in the 1980s which is still being manufactured.[24]

These changes are leading to a proliferation of unprecedented scope. The ability to acquire military vehicles is becoming a greater challenge due to civilian manufacturing for amateur use. In this niche, too, there are many manufacturers and a host of sources from which one can, for just a few hundred dollars, purchase vehicles equipped with sophisticated capabilities. The ability of civilian and military technologies to cross borders and/or be developed in nations not necessarily considered military superpowers also limits the ability to supervise the number of vehicles on the market, whether acquired by states or non-state entities.

Changing Users

The fact that many nations not only use unmanned vehicles but also manufacture and can sell them without any special restrictions means that the user base has expanded; UAV users now include non-state entities, such as terrorist and guerrilla organizations, among them Hizbollah.

Hizbollah, a Shiite Muslim terrorist organization operating in Lebanon, relies heavily on Iran in many ways. The organization operates a fleet of about 200 UAVs supplied by Iran and used for multiple purposes. Until recently, Hizbollah's use of UAVs primarily consisted of executing terror operations against Israel by means of UAVs bearing explosives. However, over the course of the past year, it has become clear that Hizbollah is using its UAVs to gather intelligence much in the same way as nations do. This, for example, enabled the organization to prevent attacks against Hizbollah targets in Lebanon- it detected and thwarted an attempt to detonate a booby-trapped vehicle.[25] Hizbollah makes similar use of its UAVs to help President Assad's forces fight the rebels in Syria,[26] and it is not the only terrorist organization that has used or is attempting to make operational use of UAVs. For instance, Hamas has been trying to acquire the capabilities to independently develop and operate UAVs for military use.[27] At least one such attempt was identified, and the UAV in question was destroyed by Israel in 2012.[28]

These two examples reflect the attempts by non-state actors to make military use of sophisticated platforms. There is evidence that they also have smaller, simpler tools that any individual could find on the internet for just a few hundred dollars. Previously, the acquisition of UAVs required a large budget and their use was limited. At present, UAVs with video and audio recording capabilities are on the market for a low price, sold to the highest bidder without inquiry into their intended use.

Changes in manufacturers and users create a significant challenge for nations attempting to preserve superiority in their airspace. Aerial defense is currently based on several aspects, as the most fundamental factor is intelligence threat assessment. In the face of extensive proliferation and the introduction of non-state actors, the challenge of ascertaining possible threats and defending against them becomes more salient. Another challenge in defending a country's airspace is balancing between civilian airspace uses and protecting against potentially harmful vehicles. Not only is the detection of a hostile vessel in one's airspace challenging, but UAVs pose an additional challenge due to their size, low altitude and low radar cross-section.

Civilian Use

One cannot ignore the extensive robotics and UAV acquisitions. Many companies have identified the commercial potential in the field, and in the past year there were numerous reports of future plans for using UAVs for a myriad of civilian applications.

The civilian market is far more extensive than the military one; its potential is huge and largely untapped. An economic research group estimated that from 2014 until 2024 the field will be worth some $89 billion.[29] This market's ability to realize this potential depends in part on legislation and regulation. AUVSI, a prominent organization in the UAV field, claims in an official report that the assimilation of UAVs in the US air traffic system (a long, complex and costly process) in a way that would allow legal, regulated and safe civilian operation of UAVs could generate some $13.6 billion for the US economy in the first three years and create 70,000 new jobs. According to the organization, every day that such a move is not made costs the US. economy some $27 million.[30]

UAVs can have countless non-military applications such as traffic and weather monitoring, search and rescue, environmental protection, firefighting, research, aerial deliveries, and various uses in communications, the press and film. These are but a few of the uses predicted for these vehicles, though the largest market today is agriculture, which may be worth some $2 billion in 2015 in the United States alone.[31]

To this effect, it seems that no nation would want to relinquish the potential benefits of this market, and the lucrative benefits of allowing UAVs to operate in non-military capacities in national airspace shall outweigh the inherent risks. Nonetheless, such operation is not self-evident and creates many challenges for any state seeking to enable it. According to the authors of the AUVSI report, there are several preconditions of which the most prominent is the development of new FAA regulations to incorporate UAVs in national airspace.[32] The dangers vary according to country, as, for instance, the US airspace is not as easily affected by the presence of UAVs while Israel must defend itself from rockets and mortars launched into its airspace, therefore the presence of UAVs may hinder aerial defense capabilities.

The most recent example of an ambitious civilian program to make commercial use of UAVs seems to be Amazon's announcement that it intends to deliver customer purchases at great speed using a fleet of UAVs. For Amazon to be able to operate a fleet of delivery UAVs, there is need for further technological progress, but the technological barrier is not the factor that will curb Amazon's ambition. Rather, laws and regulations currently restricting the use of such vehicles are liable to be a much more significant obstacle. Moreover, because Amazon is hardly the only company seeking to use UAVs, and complex regulation is needed before UAVs can be commonly used in any airspace, it will be extremely difficult to formulate legislation and regulation, not to mention their enforcement and application.

The need to regulate such issues in democratic states such as Israel, the United States, European countries and other developed nations requires a lengthy process. To regulate the field, the following components are indispensable: thought processes, legislation, regulations, creation of jobs, manpower training, and more. Such processes may take anywhere from a few months (at least) to several years, depending on the scope of regulation one seeks to effect and the amount of resources allocated to that end.

Nations seeking to regulate civilian use of UAVs must take into account several points that can be grouped into three general categories:

a. Safety: The reliability of the vehicles, separating aerial spaces and routes to prevent collisions between UAVs and prevent damage and harm to people, animals, buildings and objects.
b. Security: IFF (Identification, Friend or Foe), appropriate defenses against cyber-attacks and break-ins designed to disrupt the flight of authorized vehicles; preserving aerial preference for military and internal security vehicles in routine situations and emergencies; preserving aerial preference for civilian vehicles, conveyances of passengers and goods; preventing malicious and/or criminal use.
c. Optimal use of aerial space: Maintaining privacy and quality of life (such as the reduction of noise and other environmental impacts that the operation of UAVs is liable to produce).

Lack of Policy and Technological Solutions

It is safe to say that developments in the field of UAVs and their possible effect on threats and challenges in airspace were not sufficiently assessed in the last two decades, nor was any appropriate policy ever applied in order to prepare on the technological, regulatory or legislative levels. Support for the claim that it was possible to foresee the change and prepare for it may be found in the fact that in the military field, US forces' doctrines included references to the development of UAVs for military purposes and the additional operations this required. As part of these plans, the United States could clearly assess the potential in the field and advance and assimilate it in the FCS and BTCM a decade ago. Even if these were not fully realized, and even if they changed over the years, they were very influential in the field and included reference to a wide range of topics that require handling in order to assimilate and make use of these vehicles.

The lack of general preparation has led to a situation in which nations do not passess the technological as well as the legal and systemic solutions to confront the change currently taking place. In terms of defense against possible UAV attacks by hostile nations, non-state entities (such as terrorist organizations) or criminal outfits, there are currently few solutions providing insufficient coverage, such as the US solution – deploying laser cannons on ships in the Persian Gulf to defend against the threat of Iranian UAVs.[33] To defend larger areas, nations such as Israel train their fighter pilots to identify and bring down UAVs.[34]

Both the American and the Israeli solutions are considered problematic, particularly because of their high cost and inherent threat. Moreover, the ability to take out a hostile aerial vehicle does not depend only on having the weapons that will allow one to do so. It is also necessary to be able to identify the vehicle, to ascertain whether it belongs to a friend or a foe, and to do so within sufficient distance and time to allow a response (such as scrambling fighter jets, which requires several minutes). Currently, there are not enough of technological systems and manpower with the right training to operate them, enabling the identification of such vehicles entering and operating in one's airspace, as well as insufficient systems that can distinguish enemy vehicles from friendly ones, should a decision be made to expand the use of civilian vehicles.

Current radar systems have trouble identifying smaller vehicles flying at low altitude (a category encompassing many combat UAVs and almost all civilian UAVs freely available on the Internet). One may assume that the lack of appropriate systems is also one of the factors affecting the difficulty in allowing the operation of such vehicles in the civilian commercial market: it could be genuinely difficult to identify and follow them, as is the case today with manned vehicles.

Creating regulation and providing licenses for civilian operation of UAVs lags behind the technological feasibility, causing discontent among civilian companies and even leading to court cases against the authorities as well as to attempts to bypass the authorities and appeal to others to approve such use, which in turn is liable to lead to other dangers.[35]

Further evidence of the complexity and salience of this danger may be found in the case that was documented by television cameras in the beginning of 2014. A small UAV, of a type that may be purchased for just a few hundred dollars over the Internet, came within two meters or so of the head of German Chancellor Angela Merkel.[36] The event, which resulted in a smile on the face of the Chancellor, is a clear illustration of the fact that such vehicles are currently being operated without any authorization and are liable to represent a threat with which even the most advanced nations are unprepared to deal.

Policy Requirements

The fundamental assumptions for formulating policy include the following:

a. The existence of free commerce and the difficulty in limiting it as a result of the complete lack of current restrictions are primarily damaging to nations that are signatories to agreements in the field. By contrast, nations that are not signatories and have acquired the ability to manufacture such vehicles in recent years enjoy the current situation, leading to the opposite of the initial intention of these treaties.

b. Acceptance of the extensive proliferation of UAVs as well as a genuine difficulty in keeping up with this proliferation given the ability to build vehicles or buy them via non-state entities and turn them into platforms for espionage, explosives and more.

c. The effect of the above on non-state entities that, under current circumstances, have increasingly greater ability to buy and operate more sophisticated vehicles, posing potential danger to states and the international community.

d. The vast economic potential inherent in civilian and commercial operation. This potential raises the question: when will such operation be legally approved by states? The assumption is that no nation will want to be left behind. Any entity that prepares in time (states or companies producing solutions, both products and services) is likely to benefit significantly.

Recommendations

Given the need to confront a new reality created by the proliferation of UAVs and the desire to make use of their civilian operation, it is necessary to develop new systems with capabilities of UAV identification, location and distance retrieval. This must happen in tandem with efforts by nations, commercial companies and armies to develop or adapt existing technologies to allow for defense against UAVs operated for combat or criminal purposes. In addition, it is important that armies define doctrines and methods for dealing with aerial threats of a new type and train manpower to do so, as well as assimilate suitable tools and technologies.

Furthermore, it is necessary to act at the state and international level to enact legislation and regulation that will allow, to an extent, the regular operation of UAVs for non-military purposes (civilian and commercial) in order to enjoy their potential. To this end, nations should cooperate on international legislation in the field, defining uniform safety standards, regulating the operation of UAVs in international airspace, and preventing or keeping up with proliferation of vehicles with high potential of becoming a threat (such as armed vehicles). Adopting these recommendations and implementing them could facilitate the defense against threats inherent in these trends as well as benefitting from the advantages these trends can afford humanity.

Conclusion

The use of UAVs has been an increasing trend for the past few decades. However, their use has changed in recent years to include smaller nations and non-state organizations, a larger group of manufacturing nations, and civilian vehicles about to become operational in a wide array of applications in the next few years. It seems that the economic forecasts and the many possible applications of UAVs in the civilian market will result in increasing UAV use despite the dangers they entail and the opposition they sometimes generate.

The combination of widespread proliferation and military use or, alternately, terrorist use, as well as the many future civilian uses, will create a complex airspace arena requiring in-depth understanding and analysis to create solutions, both in the military and civilian fields. States that wish to enjoy the field and reduce the risk generated by progress must consider changes in legislation and regulation, and create technological systems and solutions and deploy them. These are lengthy processes, especially in democratic nations with organized bureaucracies.

In order to locate, create and apply the best solutions in a cost efficient manner, nations would be wise to consider cooperation in regards to international legislation and standardization of the field. States, armies and commercial companies that fully appreciate this complex challenge and that can create the technological solutions as well as assimilate them will be able to enjoy great economic advantages while minimizing the dangers inherent in the changes taking place in any case.

Notes

[1] US Department of Defense, “Directive Number 3000.09,” November 21, 2012, http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf. p. 15.

[2] Jeremiah Gertler, *US Unmanned Aerial Systems*, Congressional Research Service (January 3, 2012) http://www.fas.org/sgp/crs/natsec/R42136. p. 8-9.

[3] Ibid, p. 13.

[4] "Chapter One: Conflict Analysis and Conflict Trends," *The Military Balance*, 2014, 114:1, http://dx.doi.org/10.1080/04597222.2014.871874.

[5] United States Government Accountability Office, *Nonproliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports*, July 2012, http://www.gao.gov/products/GAO-12-536, p. 10.

[6] Isaac Ben-Israel, "The Revolution in Military Matters and Its Manifestations in the War in Iraq," in *After the War in Iraq*, ed. S. Feldman and M. Grundman (Tel Aviv, Ministry of Defense Publications, 2004), pp. 76-77.

[7] United States Government Accountability Office, *Nonproliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports*, p. 13.

[8] Ibid., p. 9.

[9] Gili Cohen, "Israel: The Biggest UAV Exporter in the World," *Haaretz*, digital edition, May 19, 2013, http://www.haaretz.co.il/news/politics/1.2023735.

[10] Mary Dobbing and Chris Cole, *Israel and the Drone Wars*, Drone Wars UK, January 2014, http://dronewarsuk.files.wordpress.com/2014/01/israel-and-the-drone-wars.pdf. pp. 19-20.

[11] United States Government Accountability Office*, Nonproliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports*, p. 13.

[12] Myrto Hatzigeorgopoulos, "European Perspectives on Unmanned Aerial Vehicles," *European Security Review* No. 63, December 2012, http://isis-europe.eu/sites/default/files/publications-downloads/esr63_perspectivesUAVs_Dec2012MH.pdf.

[13] Chris Cole, "Future Combat Air Systems: UK-France Military Declaration Reveals Development of Combat Drones," *Global Research*, http://www.globalresearch.ca/uk-france-declaration-reveals-new-reaper-users-club-to-rival-european-drones-club/5367723.

[14] Jaroslaw Adamowski, "Russian Defense Ministry Unveils $9B UAV Program," *DefenseNews* Digital Edition, Feb. 19, 2014, http://www.defensenews.com/article/20140219/DEFREG01/302190031/Russian-Defense-Ministry-Unveils-9B-UAV-Program.

[15] Brayant Jordan, "Report: China Developing Advanced Drone Fleet," *DefenseTech* digital edition March 19, 2013, http://defensetech.org/2013/03/13/report-china-developing-advanced-drone-fleet/.

[16] Ian M. Easton and L. C. Russell Hsiao, *The Chinese People's Liberation Army's Unmanned Aerial Vehicle Project: Organizational Capacities and Operational Capabilities*. Project 2049 Institute, March 11, 2013, http://project2049.net/documents/uav_easton_hsiao.pdf. p. 11.

[17] Jordan, "Report: China Developing Advanced Drone Fleet."

[18] Edward Wong, "Hacking US Secrets, China Pushes for Drones," *New York Times* Digital Edition, September 20, 2013, http://www.nytimes.

com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html?pagewanted=1&_r=0.

19 Tesfa-Alem Tekle, "Ethiopia Produces First Military Drone Aircraft," *Sudan Tribune* Digital Edition, February 14, 2013, http://www.sudantribune.com/spip.php?article45518.

20 Oscar Nkala, "Nigerian Commissions New UAV", *DefenceWeb* Digital Edition, December 19, 2013, http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=33115:nigerian-commissions-new-uav&catid=35:Aerospace&Itemid=107.

21 Edward Fox, "Colombia Producing Its Own Drones," *In SightCrime* Digital Edition, October 26, 2012, http://www.insightcrime.org/news-briefs/colombia-producing-drones.

22 Brian Ellsworth, "Venezuela Says Building Drones with Iran's Help," *Reuters*, June 14, 2012, http://www.reuters.com/article/2012/06/14/us-venezuela-iran-drone-idUSBRE85D14N20120614.

23 "Iran Unveils Biggest Missile-Equipped Drone," *al-Jazeera*, November 19, 2013, http://www.aljazeera.com/news/middleeast/2013/11/iran-unveils-biggest-missile-equipped-drone-201311182223466932.html.

24 Arthur Holland Michel, "Iran's Many Drones," *Center for the Study of the Drone at Brad College*, November 25, 2013, http://dronecenter.bard.edu/irans-drones/.

25 "Hizbullah Fleet of 200 Iran Drones Said Monitoring Syria Border," *WorldTribune.com*, November 27, 2013, http://www.worldtribune.com/2013/11/27/hizbullah-fleet-of-200-iran-drones-said-monitoring-syria-border/.

26 David Axe, "Satellite Spots Syria's Iranian-Made Drones." *Wired*, June 23, 2013, http://www.wired.com/2012/07/syria-drones/.

27 "Israel Sees Future Drone Threat from Lebanon, Gaza," *Reuters*, March 10, 2014, http://uk.reuters.com/article/2014/03/10/uk-israel-drones-idUKBREA290TJ20140310.

28 "Israel Says It Knocked out Hamas Drone Program" at *CBSNEWS* Digital Edition, November 16, 2012, http://www.cbsnews.com/news/israel-says-it-knocked-out-hamas-drone-program/.

29 "Teal Group Predicts Worldwide UAV Market Will Total $89 Billion," *2013 UAV Market Profile and Forecast*, at *TEAL GROUP Corporation*, June 17, 2013, http://tealgroup.com/index.php/about-teal-group-corporation/press-releases/94-2013-uav-press-release.

30 "The Economic Impact of Unmanned Aircraft Systems Integration in the Unites States," *AVUSI*, March, 2013, http://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/New_Economic%20Report%202013%20Full.pdf. p. 2.

31 Ibid, p. 15.

32 Ibid, p. 7.

33 Thom Shanker, "Navy Deploying Laser Weapon Prototype Near Iran," *New York Times*, April 8, 2013, http://www.nytimes.com/2013/04/09/world/navy-deploying-laser-weapon-prototype-in-persian-gulf.html?_r=0.

34 Yaakov Lappin, "Israel Air Force Pilots Practice Shooting Down Enemy Drones in Massive Drill," *Jerusalem Post*, April 30, 2014, http://www.jpost.com/Defense/Israel-Air-Force-pilots-practice-shooting-down-enemy-drones-in-massive-drill-350845.

35 Andy Pasztor, "FAA to Appeal Ruling Challenging Its Authority over Commercial Drones," *Wall Street Journal,* March 7, 2014, http://online.wsj.com/news/articles/SB10001424052702304732804579425603712376612.

36 Joe Weisenthal, "This Photo of Angela Merkel Smirking at a Drone Crash Is a Glimpse into the Future," *Business Insider*, September 15, 2013, http://www.businessinsider.com/angela-merkel-smirks-at-a-downed-drone-2013-9#ixzz31gOiyoUa.

Inter-Organizational Training for the Emergency Management System

Alex Altshuler and Meir Elran

The development and deployment of the Iron Dome system during Operation Pillar of Defense in November 2012 and Operation Protective Edge in the summer of 2014, demonstrated impressive technological capabilities. In addition, it indicated the need for an increased professionalization among the personnel engaged in emergency management, and the creation of a structured professional identity transcending organizational affiliation. Government Decision 1661 transferred the powers previously held by Israel's Ministry of Home Front Defense to the Defense Ministry. In so doing, it charged the Defense Ministry with responsibility for leading a process of strategic change in the area of inter-organizational training in an attempt to facilitate a more effective and integrative approach to addressing the major challenges currently facing Israel's emergency management system.

Keywords: emergency management system, inter-organizational training, regulation, emergency management as a professional field, strategy formulation.

Introduction

The strategic importance of the emergency management system within the national security fabric of the state of Israel is undisputed. Substantial evidence of the critical nature of this area includes the fundamental

Dr. Alex Altshuler is a Fulbright postdoctoral research fellow at Harvard University's Kennedy School of Government and a research fellow at the Institute for National Security Studies.
Brigadier General (ret.) Meir Elran is a senior research fellow at the Institute for National Security Studies, head of the Homeland Security Program, and head of the Society-Security Program of the Institute for National Security Studies.

discussions conducted in 2013 and 2014 by the government ministries claiming responsibility for, and proprietorship over preparations in this realm.[1] This extended dispute, waged primarily by the Ministry of Defense and the Ministry of Home Front Defense, concluded with Government Decision 1661 of June 1, 2014, which closed the Ministry of Home Front Defense and transferred all its powers, resources, and responsibilities to the Ministry of Defense.[2] Since the Second Lebanon War of 2006, which revealed significant failings in the functioning of the different authorities responsible for management of Israel's civilian front, Israel has witnessed numerous changes in this critical realm. Many of these changes are indicative of the current trend of improvement underway in the country's overall readiness for emergency situations.

One significant area in which progress is likely to make a substantial contribution to the formulation of an effective strategic response to the challenges facing Israel's civilian front is the training of the professional personnel affiliated with the different agencies responsible for this area: the public sector, the private sector, and the "third sector" (or the "volunteer" sector, consisting of non-government and other non-profit organizations).

Currently, most professional training conducted by the different organizations is intra-organizational and takes place within the confines of the Home Front Command, the Israeli Police Force, the Fire and Rescue Commission, The Israeli Red Cross – Magen David Adom, and other bodies. Courses and continuing education programs for officials within these organizations were also developed and conducted by the Ministry of Home Front Defense and organizations from the third sector (such as the Israel Trauma Coalition and the Cohen-Harris Center for Children at Risk). In order to effectively fulfill their purpose in this realm, the organizations that are part of the civilian front must operate in an integrative manner. The Israeli military, including the Home Front Command, conducts regular multi-organizational training programs for all the services and branches of the IDF, including specially designated training in the required areas of cooperation. However, non-military organizations do not take part in these courses. A significant development in this direction took place in February 2014 with the opening of the National Emergency Management School under the auspices of the Ministry of Home Front Defense, and following the closing of the ministry, it was incorporated into Israel's Defense Ministry. The school's purpose is to provide effective training for relevant officials within local authorities, government ministries, and other emergency bodies.[3]

The structured integration, synergy, and common language necessary for effective development on the civilian front require a systemic cooperative design. Therefore, this article offers a description and analysis of the current state of inter-organizational training on the civilian front, and offers policy recommendations for the strategic changes necessary to bring about progress.

Emergency Preparedness

Emergency preparedness requires the structured ongoing participation of a large number of organizations and groups and therefore necessitates a high degree of coordination.[4] Indeed, inter-organizational coordination and cooperation is regarded as one of the most influential factors related to preparation for states of emergency.[5] A recent study conducted in Israel indicated that inter-organizational cooperation in emergency management has played a significant and distinctive role in increasing the level of preparedness.[6] Preparation for emergency situations is inherently interdisciplinary, and therefore incorporates individuals of various backgrounds and disciplines. In order to facilitate an integrative platform, it is important to create a shared foundation.

Whereas the joint work of local authority officials and national government agencies is addressed by legislation,[7] there is no such regulation or legislation regarding non-government organizations and their integration into emergency management schemes. The current trends of expanded involvement of the third sector,[8] privatization, and outsourcing[9] also appear to be heightening the importance of the joint effort of local authority officials and a variety of non-government civil bodies to achieve optimal preparedness for emergency situations. This, however, has been accompanied by the formidable challenge of creating a common language between the diverse and complex mosaic of the parties involved, with an eye toward achieving effective integration of government and non-government forces. During the Second Lebanon War, non-government agencies were intensively involved in a diverse range of activities aimed at providing assistance to the affected communities and their varied and multi-dimensional needs.[10] Nonetheless, no mechanism for coordination between government and non-government agencies was established with regard to this wartime work on the national and the local level, and this had a detrimental impact on the ultimate effectiveness of the response in the civilian realm. The effort to meet the changing needs of the civilian population during the war was more comprehensive and effective in local authorities, in which more meaningful collaborative work had been conducted and in which there was greater coordination between all the involved parties.[11] Indeed, as a result of the process of formulating the lessons from the Second Lebanon War, during Operation Cast Lead the "third sector" organizations and relevant stakeholders from the private sector played a role in providing assistance to the civilian population and state officials led daily "roundtable" discussions aimed at formulating effective integrated working methods for all the parties involved.

It is important to emphasize that cooperation in such contexts must not be limited to ongoing emergency situations. Indeed, the need for local inter-organizational and inter-sectorial cooperation in preparation for emergencies was one of the major lessons learned from Hurricane Rita and Hurricane Katrina in the United States.[12] That being the case, the achievement of inter-organizational synthesis, which requires ongoing theoretical and applied joint-training for relevant officials within all the organizations involved, must be regarded as an essential element of preparing for and contending with states of emergency.

Inter-Organizational Training on the Israeli Civilian Front: Current State of Affairs, Trends, and Processes

The two major agencies with relevance to inter-organizational training on the civilian front in Israel are the IDF's Home Front Command and the Ministry of Home Front Defense. The following assessment of the developments currently underway in inter-organizational training in Israel is based on the analysis of professional materials, political trends, and meetings of the authors with relevant officials during the years 2012-2014.

a. There is currently no integrative national conception accepted by all relevant parties and no one agreed-upon professional authority for training the civilian front, possessing the power to determine required and comprehensive content and training frameworks and to supervise the implementation of training programs conducted by different organizations. There is, however, an understanding of the importance of inter-organizational training, as reflected in the establishment of the

National Emergency Management School and the implementation of interdisciplinary training programs by the Home Front Command. The need for integrative inter-organizational training was classified by the Ministry of Home Front Defense in its summary for 2013 as one of the main lessons learned during the year and as a major issue to be dealt with in 2014. However, without a solid legislative foundation and without cooperation between the major stakeholders involved, a sustainable "quantum leap" in this area will remain unattainable.

b. In the course of 2012-2013, the Ministry of Home Front Defense considered the establishment and operation of inter-organizational training courses. Another option discussed was the possibility of granting civilian training bodies (universities and colleges), and their programs of study, official recognition by the Ministry of Home Front Defense. In this context, officials discussed the possibility of authorizing the content of both academic programs (programs of study for the purpose of earning bachelor's and master's degrees in the field of emergency management, which have existed in institutions of higher education in Israel for a number of years) and non-academic continuing education programs. Nonetheless, in 2014, the Ministry of Home Front Defense decided to run the National Emergency Management School on its own and abandon efforts toward "certifying" external training bodies, at least for the time being.

c. In addition to inter-organizational training programs which focus primarily on promoting professional cooperation, another important matter is the provision of required professional training for relevant officials within the different systems involved in emergency management. For example, within the local authorities, there is still no obligatory training program for emergency managers pertaining to the specific issues involved with emergency management during different types of situations. This training is extremely important given the fact that many local emergency managers do not have academic background in that field. The same is true of many relevant officials within government ministries and other bodies. The Ministry of Home Front Defense had begun to bridge this gap within government ministries and other emergency organizations. The first inter-organizational continuing education program for senior level personnel began in February 2014 and concluded the following month in the framework of the National

Emergency Management School. However, The IDF's Home Front Command refused to take part in this training program.

d. The IDF Home Front Command intends to expand training and information dissemination within different sectors. The differentiated work characterized by cultural sensitivity. In this context, initial efforts have been conducted in training civilian volunteers for emergency activity in the Arab communities and the Jewish ultraorthodox sector. In the Arab sector, the Home Front Command, in cooperation with the Israel Trauma Coalition, conducted training for social workers (including a course specially designed for the Bedouin community) that has generated interest in further collaboration. Attention to people with special needs has been manifested in an additional training course organized by the Home front Command – for superintendents of "supportive communities" for the elderly and special needs populations run by JDC Israel and the Ministry of Welfare and Social Services.

e. The Home Front Command has recently begun to reach out to citizens to elicit their assistance during states of emergency, based on recognition of the essential role of civilians in initial search and rescue efforts in the wake of disasters. In this context, the Home Front Command, Magen David Adom, and the National Fire and Rescue Commission have developed an integrated training program known as "First Self-Aid" in local authorities throughout the country. This course is aimed primarily at providing participants with the capability to independently begin rescue operations in the wake of an earthquake.

f. There is a growing recognition that emergency management is a distinct professional field and discipline requiring specialized training and specially designed academic education. One of the long-term challenges with which it will be necessary to contend in order to provide a complete solution for such training programs is the absence of legislation and regulation of the field of emergency management within the framework of the "Home Front Law" (different versions of which have been discussed by Knesset committees since 2008). Among other things, this law should define the mandatory terms for licensing individuals working in the field of emergency management and institutionalize procedures for licensing the institutions engaged in education and training in this field.

g. In the current situation, most emergency management organizations provide independent training, and the National Emergency Management School was established in an effort to improve this state of affairs. In addition, the Home Front Command integrates representatives of other bodies into its training courses (such as its district commanders' course and its course for commanders of liaison units to local authorities). Still, it is important to remember that, first and foremost, these courses were planned and structured to meet the needs of the Home Front Command itself. The district commanders' course includes representatives from the Israeli Police Force, Magen David Adom, Fire and Rescue, security officers and emergency supervisors, and senior local authorities officials. The Home Front Command's courses for its company and battalion commanders are also attended by representatives of the Israeli Police Force, Magen David Adom, and chief emergency managers of the local authorities. The Home Front Command developed training programs specially designed for specific stakeholders on the civilian front, such as civil defense coordinators. This course–which is attended by representatives of the local authorities, government ministries, and business enterprises–has been offered on a regular basis since 2007.

h. In spite of the absence of an institutionalized system of basic inter-organizational training programs, a comprehensive system of drills, exercises, and management simulations–in which representatives of the different organizations operating on the civilian front take part–has existed for a number of years. Most of these exercises are inter-organizational by nature, as defined by Procedure No. 15 of the Emergency Economy System (MELACH), which relates to the issue. This system of inter-organizational exercises includes annual drills for most of the local authorities in Israel, exercises within government ministries, integrated national exercises, and an annual national emergency week revolving around the national home front exercise that has been conducted since 2007 with a focus on specific types of emergency (earthquakes, non-conventional weapons' attacks, etc.).

Policy Recommendations

In general, awareness of the issues related to emergency management appears to have increased significantly in government ministries and among relevant officials within local authorities. On this basis, a path is paved for the promotion and development of inter-organizational training. Beyond the realm of any specific training, there appears to be consensus among senior elements on the civilian front regarding the need for the establishment and development of a system of inter-organizational training programs for the different bodies operating in the field of emergency management. This agreement stems from the recognition that no single agency or body is capable of contending with the ever growing challenges, as well as an understanding that the constant strengthening of inter-organizational operational cooperation is a key to success. However, the organizational culture of the civilian front today is tainted by a high degree of unnecessary competition over credit and prestige, contributing to a bitter and ever intensifying dispute over seniority among the different bodies operating in the field of emergency management. This, of course, has had a detrimental impact on the promotion of integrative training programs.

The system of inter-organizational training in Israel is still in its infancy, but the establishment of the National Emergency Management School in 2014 has been an important development. In addition, an emerging fundamental conceptual difficulty lies in the fact that even if representatives of these bodies are aware of the fact that they are required to work in close cooperation with one another and that this necessitates joint training and exercises within a framework of integrative activity, each, in practice, relies on different bodies of knowledge and their own experience and tradition. For this reason, this work cannot be based on a common professional "melting pot," as is the case, for example, In the IDF'S inter-branch collaboration. The civilian front also undoubtedly requires a wise and dynamic combination of intra-organizational and inter-organizational training.

On this basis, the subject of inter-organizational training is closely linked to three strategic efforts that must be pursued on the civilian front: legal and organizational regulation in the field of emergency management on both the national and local level; formulation of an integrated operational conception with authority over all the relevant parties; and recognition of emergency management as a unique professional field.

Although the need for legal order is accepted in principal by all, obstacles stemming from organizational factors and narrow interests have been hindering its implementation since 2008. The absence of an integrated operational conception is rooted in inter-organizational competition, as the essential documents of each body, drawn up in accordance with its particular point of view, are often unacceptable to or at odds with the views of other bodies. No solution to this problem can be expected until normalization of the relationship between the relevant bodies is achieved. As for recognition of emergency management as a professional field – this requires further investigation and clarification.

Though the issue has been the focus of deliberations and evaluations, more substantial work-based momentum is still necessary on all levels, as the issue stands to have far-reaching impact on the effectiveness of work on the civilian front.

It is important to remember that in addition to the officials whose professional field is emergency operations, there are many other officials who are usually not connected to the field of emergency management, but are "activated" in case of emergency. In order to facilitate their effectiveness, it is necessary to map them into three sectors (public, private, and the third sector) and to build appropriate frameworks for their training. It is also necessary to recognize the unique professionalism of the field of emergency management, as well as to establish a comprehensive system of fundamental academic study and ongoing integrative training and instruction based on an agreed upon operative conception, joint multi-year working plans, and calibrated inclusive mechanisms of implementation. Israel's defense establishment, which was imbued with the primary powers pertaining to the civilian front by Government decision 1661 of June 1, 2014, now faces a number of questions of major significance in the realm of training:

1. In addition to the public sector, how can all the other relevant parties– on the municipal level, in the private sector, and in the third sector– be incorporated into the joint effort?
2. Which professional areas shall be incorporated into the professional identity of the field of emergency management and which shall remain within related fields and be worked with in close cooperation? What expertise will be defined as integral to the new field?
3. What are the minimum requirements of those seeking certification to work in this field?
4. What academic, inter-organizational, and intra-organizational levels will make up the ladder of professional development for those engaged in the field of emergency management?

In order to provide thoughtful and in-depth answers to these questions, it will undoubtedly be necessary to carry out a process of change aimed at the creation of an integrative whole that is not a product of organizational patchwork, that possesses its own internal consistency, and that facilitates the necessary "strategic quantum leap."

In conclusion, in addition to the cultivation of technological-operational capabilities so impressively demonstrated in the development and deployment of the Iron Dome system during Operation Pillar of Defense in November 2012 and Operation Protective Edge in the summer of 2014, from which the civilian front clearly benefited, it is necessary to increase professionalization among the personnel engaged in the field of emergency management, and create a structured professional identity in this field that transcends association with any one specific organization.

In 1952, Major General (Res.) Aharon Yariv was appointed to head the team that established the IDF Command and Staff School. Today, there is an urgent need to establish a comparable body on the civilian front – one that is accepted by all the parties involved and that is capable of playing a key role in a broad new training system. This task is as challenging as it is necessary and should be pursued without delay.

Notes

[1] For example, see the discussions of the Subcommittee of the Knesset Foreign Affairs and Defense Committee on Home Front Preparedness from February 27, 2014 and March 13, 2014 http://main.knesset.gov.il/Activity/committees/ForeignAffairs/News/Pages/pr_270214.aspx.

[2] Government Decision No. 1661, Transfer of the Home Front Defense Ministry's Field of Operation to the Ministry of Defense, June 1, 2014, http://www.pmo.gov.il/Secretary/GovDecisions/2014/Pages/dec1661.aspx.

[3] See the Israel Defense website, "School for Emergencies," February 5, 2014 http://www.israeldefense.co.il/?CategoryID=483&ArticleID=5810.

[4] Lori A. Peek and Jeannette N. Sutton, "An Exploratory Comparison of Disasters, Riots and Terrorist Acts," *Disasters* 27, no. 4 (2003): 319-35.

[5] Thomas E. Drabek, "Community Processes: Coordination," in *Handbook of Disaster Research* (New York: Springer, 2007), pp. 217-33.

[6] A. Altshuler, *Emergency Preparedness of Local Authorities for War-Caused Disaster: The Israeli Case*, Master's thesis, University of Haifa School of Social Work (2008).

[7] See, for example, The Civil Defense Law, 1951; The Municipalities Ordinance, 1973; and The Local Councils Order, 1972.

[8] B. Gidron and Y. Elon, *Database Report 2007: Patterns and Changes in the Third Sector in Israel in the Past Decade*, Ben-Gurion University in the Negev, Israeli Center for Third Sector Research, 2007; B. Gidron, M. Bar, and H. Katz, *The Third Sector in Israel: Between Welfare State and Civil Society* (Hakibbutz

Hameuchad, 2003); Yael Yishai, "Civil society in transition: interest politics in Israel." *The Annals of the American Academy of Political and Social Science* 555, no. 1 (1998): 147-62.

9 D. Dekel, *The Second Lebanon War – The Lessons of the Regional Councils*. Regional Councils' Center (2007); S. Azriel, *The Local Authority – Home Front and Battlefront?!* A Report for the Prime Ministerial Conference on Local Government (2007).

10 Ira Sharkansky, "Local Autonomy, Non-Governmental Service Providers and Emergency Management: An Israeli Case," *Journal of Homeland Security and Emergency Management* 4, no. 4 (2007); E. Ben-Harush, *The State's Responsibility toward the Weakened Citizen during the Second Lebanon War: The Elderly and the Disabled as a Case Study*. Graduation Paper, IDF College of National Defense (2007).

11 H. Katz, E. Raviv, H. Yogev, M. Yaacobi, E. Levinson, Y. Elon, and B. Gidron, *Israeli Civil Society During the Second Lebanon War*, Ben-Gurion University in the Negev, Israeli Center for Third Sector Research (2006).

12 Gloria Simo, and Angela L. Bies, "The Role of Nonprofits in Disaster Response: An Expanded Model of Cross-Sector Collaboration," *Public Administration Review* 67, no. s1 (2007): 125-42.

Protecting Foreign Manpower in the Israeli Gas Industry: Lessons from Nigeria

Elai Rettig

Global experience with oil and natural gas production indicates that international energy companies do not refrain from operating in areas of conflict and are not easily deterred by periodic terrorist attacks on their facilities. However, the case of the Nigerian Movement for the Emancipation of the Niger Delta (MEND) shows that even large corporations are liable to close their facilities when there is a direct attack on their foreign (non-local) employees. Israel can learn from the Nigerian experience how to cope with the vulnerability created by its dependence on foreign employees and consequential threats directed against its natural gas resources. A short term lesson is that Israel must ensure the safety of employees in its Exclusive Economic Zone (EEZ), even when they are employed by a foreign company that is obligated to protect them. A long term lesson is that Israel must reduce its dependence on foreign experts by training a local workforce that may be less affected during times of national crisis.

These aspects are as important for Israel's energy security as the facilities' physical protection.

Keywords: Energy security, energy policy in Israel, natural gas infrastructure, terrorist threats, international terror, foreign employees, protection of employees

Elai Rettig is a doctoral candidate at the School of Political Science at the University of Haifa. He holds a research scholarship from the Ministry of National Infrastructures, Energy, and Water Resources and a President's Scholarship from the University of Haifa.

Introduction

The Israeli defense establishment is currently assessing possible threats to natural gas production and export facilities that are scheduled to be built in Israel and in Israel's Exclusive Economic Zone (EEZ). In their initial phase, these facilities include drilling rigs and intermediate platforms, followed by production facilities, underwater pipelines, and onshore gas reception facilities. In the future, they will probably include land or sea facilities for producing Liquefied Natural Gas (LNG) for export. The various facilities will be mainly managed and operated by a number of foreign corporations. Currently these include Noble Energy, an American company, which is already operating the drilling and production facilities at the Tamar and Leviathan natural gas fields, and Edison, an Italian company, which has joined Israel's Delek Corporation in implementing a number of exploration licenses. In addition, Woodside Petroleum, an Australian company, was until recently signed on to operate the future gas liquefaction facilities.[1] Like the employees in the Yam Tethys production facilities,[2] the vast majority of those who operate and maintain the Tamar and Leviathan drilling rigs for Noble Energy are not Israeli citizens; they are a small group of American and Eastern European engineers and professionals. It is reasonable to assume that the majority of personnel who will operate and maintain the future liquefaction facilities (whether operated by Woodside Petroleum or another company) will not be Israeli citizens either, due to the unique expertise required to operate an advanced gas liquefaction project and the significant shortage of manpower for energy and gas engineering in Israel.

Meanwhile, the Israeli defense establishment is preparing to provide the many security measures required for ensuring the safety of the production and export facilities throughout their construction, as well as during their operation. Most of the preparations focus on protecting the physical infrastructure connected to the regular production and export of natural gas (pipelines, rigs, onshore reception facilities, and the like). At a conference held by the Institute for National Security Studies in November 2010, Brigadier General (ret.) Noam Feig, former deputy commander of the Israel Navy, presented a list of possible threats to infrastructure posed by hostile states and terror organizations. The threats included firing of missiles at gas reception facilities along Israel's coast during wartime, underwater pipeline sabotage, hostile aircrafts deployment to the high seas, and detonation of production facilities using naval vessels.[3] Nevertheless, an important subject that appears to have thus far been neglected is the manpower involved in operating the facilities, and in particular, those in Israel's EEZ, outside the borders of the country.

Counter to popular perception, large oil and gas companies are not easily deterred from working in areas of conflict, despite repeated attacks on their physical infrastructure. The reason for this resilience is that these companies take into account acts of sabotage against their production and export facilities, whether directed against the facilities themselves or the pipelines attached to them. American, French, Italian, and British energy companies operating in high-risk areas, such as Iraq, Nigeria, the Ivory Coast, or the Congo, usually display a relatively rapid return to full production following such events. The case of Iraq is especially instructive; in 2013 alone, a central pipeline carrying oil from the Kirkuk field in the Kurdish region to the port city of Ceyhan in Turkey was bombed thirty times.[4] Though these incidents led to a significant decrease in the flow of oil from northern Iraq, the pipelines were repaired very shortly after and the companies continued to operate in Iraq throughout that year.

State-owned national oil companies are better equipped to weather the storm of a national or international crisis, as can be seen in the case of the 1980-1988 Iran-Iraq War. Despite repeated attacks carried out by the Iraqi Air Force specifically targeting Iran's oil industry, Iran was able to continue production and export of large quantities of oil. Iran's success was the result of carefully planned infrastructure, including high redundancy of pipelines and facilities, as well as a competent and resilient local workforce that was able to work under fire and quickly rebuild the damaged infrastructure.[5]

Notwithstanding their remarkable resilience and speedy return to normal following sabotage, it seems that the international oil and gas companies' Achilles' heel lies within its workforce. Global experience indicates that when faced with clear and present danger, Western production companies (especially in north and central Africa), tend to avoid risks involving direct harm to their employees. Such companies have been known to suspend their activities in light of danger to their employees, even though they may breach their contractual obligations to the host country. Such danger to the workforce may be caused by an eruption of a violent conflict in the host country or specific attacks carried out by extremist groups, targeting the company's employees and executives. Temporary shut-downs significantly reduce output over time, and may cause the companies to condition their continued operations upon concrete security guarantees given to them by the host country.[6] This so-called "weak spot" is not only a result of the management's responsibility to its employees; it is also a result of the great difficulty in persuading foreign experts to remain in the host country when their lives and the lives of their families are in danger, as well as the difficulty to replace foreign experts and provide insurance coverage for the period of time they spend in the production facility.

This issue is especially pertinent when examining the Israeli case, since its dependence on foreign companies and experts for operating its gas industry exposes it to threats that could paralyze gas infrastructures, even without direct physical harm. These threats are further emphasized by the international nature of the organizations that operate against Israel. In the past, these organizations were shown to have the ability to strike Israeli and Jewish targets overseas, whether they were official targets (Israeli embassies and Jewish institutions around the world), unofficial targets (Chabad houses and Israeli tourist groups), or individuals (Israeli ambassadors and delegates). These organizations' proven ability and willingness to operate outside of Israel makes Israel's dependence on foreign employees for producing its natural resources especially sensitive.

The potential threats facing companies such as Noble Energy or Woodside Petroleum due to their activity in Israel could involve attacks against their branches and facilities in various locations around the world (West Africa, East Asia, and South America), or even individuals, such as employees and senior managers. Even a direct verbal threat made against specific targets connected to these companies would be sufficient to potentially obstruct continued operations in Israel, and to spur new demands by the companies to ensure their safety (which would also entail additional implications for the Israeli economy). It is reasonable to assume that these demands would increase precisely in times of emergency such as an eruption of war, when the continued production of gas for electricity would be the most crucial.

The problematic nature of Israeli energy dependence upon foreign companies has proven to be critical at times of crisis. In 2006, during the Second Lebanon War, foreign ships and oil tankers refused to dock in the port of Haifa and deliver fuel to Israel's refineries (Oil Refineries Ltd. – ORL) because the state did not guarantee insurance coverage in the event of collateral damage. Given the fact that Israel could not force any ship to anchor in its ports under fire, and since it did not have oil tankers of its own, the Israeli Air Force suffered from a fuel shortage towards the end of the war. This strategic weakness resulted in a report issued by the state comptroller, who demanded in 2008 that ORL purchase an oil tanker and prepare an Israeli crew to operate it in order to ensure regular fuel import even during times of emergency.[7]

The events of the Second Lebanon War clearly demonstrated the potential danger posed by the excessive reliance on a third party. This danger is exacerbated when discussing Israel's natural gas resources, since by 2020 production of 70 percent of the country's electricity will rely on these resources. The fact that such a fundamental component of the Israeli electricity sector is based on foreign expertise exposes Israel's economy to harm which is not evident in other locally-managed infrastructure in the country (such as water and communications). It appears that lessons have indeed been learned since the Second Lebanon War in regards to Israeli maritime transport procedures, and a similar move must be made in the Israeli gas industry as well.[8]

The case of Nigeria's oil and gas industry can be used to demonstrate the great vulnerability created by dependence on outside expertise to operate and produce natural resources. The Nigerian oil and gas industry's bitter experience coping with the militant Movement for the Emancipation of the Niger Delta (MEND) serves as an important case study. MEND's success in paralyzing parts of the Nigerian oil industry since 2006 is a result of its choice to directly attack the large oil and gas companies' foreign employees, rather than just focusing on their physical infrastructures, as has been the common practice among other groups in the region. Despite evident disparities between the two countries in question, the case of Nigeria can provide Israel with indications to the regular response patterns of Western oil and gas companies in cases where there is a clear danger to their employees.

Through an examination of the Nigerian case, this paper will suggest a number of possible ways of facing these threats, both in the short term and in the long term.

The Case of MEND in Nigeria

Nigeria is the largest oil producer in Africa and the fifth largest oil exporter in the world, with some 2.3 million barrels of oil exported a day.[9] It has also been an official member of OPEC, the Organization of the Petroleum

Exporting Countries, since 1971. In addition, Nigeria possesses proven reserves of some 5,100 BCM (billion cubic meters) of natural gas, ranking it ninth in the world and the fifth largest global LNG exporter, with exports of some 25 BCM in 2010 alone. Exports of oil and natural gas constitute approximately 40 percent of government revenues and some 95 percent of the country's earnings from exports. Consequently, Nigeria is completely dependent on this industry for balancing its annual budget.

Most of Nigeria's active oil and gas reserves are located in the Niger Delta region in the south of the country, a swampy area whose residents suffer from grave poverty. The oil and gas fields' development creates serious pollution and harms the local agriculture and fishing industries which constitute the local residents' livelihood. Development and production is carried out through a Production Sharing Agreement (PSA) between the Nigerian National Petroleum Company (NNPC) and international oil and gas companies operating in the country. These include Shell, which produces some 1.2 million barrels of oil a day; ExxonMobil, which produces some 800,000 barrels a day; Chevron, which produces some 500,000 barrels a day, as well as Total and Eni.

Most of the oil and gas fields in Nigeria are located on shore and in shallow water, though since 2003, the country has also begun deep water production at a rate of 800,000 barrels of oil a day. While it is the fifth largest LNG exporter in the world, Nigeria's vast gas reserves remain largely unexploited, and some of the gas is even burned in order to speed up oil production in areas where gas and oil are mixed.

Notwithstanding the extent of its export activity, Nigeria is far from exploiting its full production potential due to an ongoing state of insecurity and instability. For many years, the oil and gas industry suffered violent attacks by local armed groups in the Niger Delta region, demanding rights, money, or independence for the province. These attacks mostly included oil theft through pipeline sabotage (also known as "bunkering," a practice that continues to this day), pipeline bombing, and takeover of production facilities, which temporarily decreased activity. Although these attacks were numerous, they did not achieve their long-term objective since companies were able to quickly repair the damage, and Nigeria's overall annual production rates were hardly affected.

This situation changed in 2006, with the appearance of the MEND militant group, calling for a redistribution of oil profits in the country and for greater independence for residents of the Niger Delta region. The group's success in promoting its objectives stemmed from the new tactic it adopted against foreign oil and gas companies. MEND, unlike other organizations, chose to focus on the foreign employees operating the facilities rather than the facilities themselves. The organization's actions included abducting Western oil and gas employees (particularly from the United States, Great Britain, France, and Japan), murdering local employees, torching the homes of foreign managers, threatening company executives, and making numerous demands for ransom.[10]

MEND first made headlines following the abduction of four foreign employees from Nigeria's shallow-water drilling rigs in January 2006. In the same month, it had also attacked a production facility and killed 17 employees. Following that attack, it issued an e-mail stating "It must be clear that the Nigerian government cannot protect your workers or assets. Leave our land while you can or die in it." It added that "our aim is to totally destroy the Nigerian government's ability to export oil."[11] MEND continued to make use of guerilla tactics including firing machine guns from motorboats and detonating dynamite. In its first year, the organization managed to cause extensive damage to the Nigerian oil industry, resulting in a decline of some 400,000 barrels of oil a day in the country's general production.[12] Between 2007 and 2010, MEND was responsible for 114 employee abductions and approximately 200 murders,[13] and in 2010 alone, it abducted 64 employees.

The deliberate attacks on international oil and gas companies' employees resulted in closing the facilities located in the Niger Delta region for lengthy periods, evacuating foreign employees from Nigeria, and declaring "force majeure" in their production and export contracts both with the host-country and the various importers. Shell and Chevron became main targets for attacks by MEND because of their extensive operations in the area, and since 2006 several of their facilities have been permanently shut down. Plans for continued expansion of production in the oil fields have been abandoned for a long period, as have plans to develop the extensive natural gas fields discovered in the region. A number of smaller oil companies have completely discontinued their operations in Nigeria, while large international companies have notified the government that the continued oil production is conditioned upon their employees' safety.[14]

Since 2006, the repeated attacks on oil facilities have led to a 25 percent decline in Nigeria's average production and export rate, even reaching a 40 percent reduction, translating into almost one million barrels a day.[15] Thus, for example, of an estimated production potential of 2.9 million barrels a day, in 2009, Nigeria produced an average of only 2.2 million barrels a day. Of all the foreign companies operating in the region, Shell suffered the most serious damage to production capacity, seeing as most of its facilities are located on shore or in shallow water. While its maximum production capacity was estimated at 1.3 million barrels a day, in 2011, it was able to produce a little less than 1 million barrels a day.

Natural gas production capacity in Nigeria was also severely affected, especially after Shell closed its large Soku plant that had come under attack in 2008. The company was only able to reopen the plant five months later, partly because of difficulties in recruiting and insuring outside experts, and it did not return to its original rate of production until 2010. As a result, during 2009 Nigerian LNG exports dropped by 33 percent.

The unstable supply also led to a lack of confidence among importing countries regarding Nigeria's ability to keep its export commitments. The United States, the largest customer for Nigerian oil, reduced its imports from Nigeria from about 1.1 million barrels a day in 2005 to 800,000 barrels a day in 2009. The decrease was partly caused by the Shale Oil and Gas Revolution in the United States, which reduced dependence on oil imports and allowed the country to give preference to more stable sources of oil than Nigeria.

Over the years, the Nigerian government's efforts to launch a military strike against MEND were futile. The harsh swampy terrain in the Niger Delta and MEND members' familiarity with the area have circumvented several military strikes. In 2009, the government attempted to sign an amnesty agreement with MEND, with OPEC's mediation. The agreement included disarming the organization in exchange for payments for its members' rehabilitation and reentry into society, as well as the restoration of civilian infrastructure in the Niger Delta region. Although the agreement was officially signed, it was not fully implemented due to Nigeria's failure to provide the required payments, and MEND resumed its operations in early 2010. As a result, the Nigerian government submitted a formal request to the United Nations to establish a commission to recommend ways of handling the organization, and foreign oil companies realized that they must provide security for their employees through private companies pending a sustainable solution.

Since 2011, MEND has reduced the frequency of its attacks against Chevron and Shell, and a number of reports have speculated the reason being "protection money" paid to the organization by the companies themselves. MEND serves as one of the "security companies" hired to protect these facilities. A special report issued in 2012 by an independent organization called "Platform" claimed that in 2009, Shell alone was forced to pay some $75 million to MEND and similar organizations for "security purposes."[16] This solution is not unreasonable in Nigeria, where even the government itself occasionally signs "security contracts" with heads of local militias in exchange for peace.[17]

Another unexpected problem resulting from MEND's violent actions is connected to human rights and environmental organizations speaking out against the international oil companies operating in Nigeria. Since the beginning of MEND operations, allegations of widespread pollution in the Niger Delta area and harm to the residents' livelihood have received greater exposure in the international media, raising awareness of the area's dire state. The reports on protection money have also provoked harsh reactions among human rights' organizations, arguing that the international oil companies are actually funding the violence in the area by making payments to the organizations that perpetrate it.[18] It should be noted that though the international companies' image had arguably suffered a blow, their operations in Nigeria remained unaffected.

Lessons for Israel

The Nigerian experience illustrates the ways in which violent organizations can significantly disrupt a country's production and export of natural resources. MEND's success in hindering the Nigerian oil and gas industry's operations since 2006 indicates the Western energy companies' vulnerability when facing direct and prolonged attacks against their employees. Chevron and shell's response to the threats against them shows that even the largest oil and gas companies will not hesitate to close their facilities and breach their contractual obligations when their employees become a target, while smaller companies completely stop their operations in the country.

These companies' response patterns should be studied by Israel, since the tensions between the Nigerian government and the international oil and gas companies, which ultimately led to a breach of the contract between them, have arisen in the wake of attacks on their personnel, not their facilities. Specifically, they have raised the question of who is ultimately responsible for the employees' safety. This question must also be at the center of discussions in Israel. Experience shows that if the foreign company fails to provide appropriate protection, the host country will suffer the consequences, and ultimately, it will be forced to take this role upon itself. This principle is especially evident in the case of Israel; if the foreign employees abandon the gas production facilities during emergencies, Israel, whose electricity production depends on gas, may suffer a serious crisis. In such a crisis, the government and military may be forced to intervene, regardless of the presence of alternative security measures such as private security firms. The many threats from terror organizations to Israel's gas reserves (whether or not they are fulfilled) emphasize the need to provide government guarantees for protecting the personal security of foreign employees in Israel's EEZ.

It should be noted that Israel and Nigeria present quite different cases in terms of threats; while Israel's production facilities are in the sea, not on land or in shallow water, making them a more difficult target, most of the attacks against personnel in Nigeria have taken place within the country's borders (aside from a number of threatening messages sent to the foreign companies' executives). Unlike Nigeria, the scope of the threat to foreign companies operating in Israel is not limited to Israeli soil. In addition, the threats posed to Nigeria by MEND cannot be compared to those posed by organizations such as Hizbollah and Hamas to Israel, since the nature of their activity, their internal organization, and their declared goals are very different. The involvement of external actors in acts of terror against Israel also adds a unique dimension. For example, because Hizbollah is located in Lebanon, this turns any action it carries out against Israeli gas facilities (or alternatively, any retaliatory action by Israel against Hizbollah) into an international incident, while a similar military action by Nigeria against MEND would be considered suppression of a local uprising.

As noted before, Israel's security establishment is currently assessing the possible threats to the natural gas industry facilities located in its EEZ, as well as to those that may take place on land and in its sovereign waters. Hizbollah, which has already expressed its intention to target the Tamar and Leviathan gas fields,[19] is a key threat, as it can control Lebanon's maritime border with Israel.[20]

Israel's gas and oil production will rely on two international companies: the American Noble Energy and Australian Woodside Petroleum, both of which significantly depend on foreign employees to operate their rigs and infrastructure (it is reasonable to assume that in the future this will also be the case in the exploration industry in Lebanon). This makes the threat profile for Israel especially high due to Hizbollah's capabilities which include possible attacks targeting foreign executives and employees while they are abroad; attacks on the companies' facilities in other areas of operation around the world (for Woodside Petroleum, facilities located in South Korea, Peru, and Brazil,[21] and for Noble Energy, facilities in Cameroon, Equatorial Guinea, Sierra Leone, Nicaragua, and the Falkland Islands);[22] and attacks on various offices around the world (Woodside Petroleum's branches in Australia, East Timor, South Korea, China, and Japan and Noble Energy's branches in the United States, South America, West Africa, and London). A personal attack on company employees and managers, while they are in the United States or Europe, appears less likely. However, their operation in regions such as West Africa, South America, and East Asia—areas in which Jewish and Israeli targets were attacked in the past—further complicates the situation. The very fact that a terrorist organization like Hizbollah is making explicit, public threats against foreign companies' executives (for example, threats that mention them by name and give their address, as had happened in Nigeria) could lead to increased tension and a demand for greater security guarantees from the state as a condition for continuing their operations in Israel. Furthermore, a threat against the employees themselves could complicate their stationing in Israel due to insurance considerations, as well as a demand by companies to reopen existing contracts with the state in order to cover additional costs. If threats are carried out—such as a threat to detonate a production facility belonging to the company in Africa, or to sabotage one of its branches around the world—this could later lead to the suspension of operations in Israel. At least theoretically, an organization such as Hizbollah could thus cause significant damage to Israel's gas production and export capabilities, even without striking any physical gas infrastructure within the borders of the state of Israel.

Nigeria's bitter experience since 2006 and the threat profile faced by Israel indicate that when a state is dependent on foreign production companies (and even more importantly, foreign employees) to produce the energy resources in its possession, it must place an emphasis not only on protecting the physical production infrastructure in its territory (pipelines, reception and export facilities), but also the safety of the foreign employees operating them outside its territory. Israel's options for providing such protection can be divided into two time periods: In the short term, the state may pay for foreign employees' protection, or at the very least, supervise it, since in the event of a crisis the state will be forced to absorb the damage and find a solution. It appears that in this case, economic considerations dictate a preference for immediate and controlled expenditures on manpower security over a future risk of incalculable damage to the electricity sector. Such protection must include personnel working in facilities while they are in Israel's exclusive economic zone or sovereign waters (as is the case on existing rigs), and possibly also include the foreign companies' offices and facilities around the world, as well as their executives. It is likely that this protection will involve hiring third-party services.

Although it can provide physical protection from attacks, it appears that there is little Israel can do to prevent verbal threats made by terror organizations against foreign companies and their officials outside of Israel. The unofficial solution to this issue adopted in Nigeria is paying protection money in exchange for their employees' safety. The Israeli defense establishment will probably refuse to discuss such a course of action, even though it might be acceptable to the foreign companies themselves.[23]

Another option for ensuring employee safety comes in the form of cooperation with Lebanon on exploration licenses. This option assumes that if companies engage in resource exploration and production in Israel and Lebanon, linkage may be formed between the facilities on both sides, wherein an attack on facilities in one country may affect the operation of the facilities in the other. A similar solution could appear in the form of sharing reserves, in which Israel would export part of its gas to the Palestinian Authority and Jordan, thus turning the gas reserves' security into a regional interest.[24] Such decisions could provide a long-term and effective solution, exceeding that of a purely military approach, which would be focused on protecting Israeli gas facilities through a "balance of terror" in which every threat or action against Israeli facilities would be met by a similar Israeli response against gas facilities in Lebanon. Such an approach cannot be considered as a long-term solution since even if Lebanon is able to establish natural gas production facilities on its soil,these will be owned and operated by international companies. Therefore, it is highly unlikely that Israel would retaliate by attacking American, French, or Russian facilities on the Lebanese side.

In the long run, Israel can significantly reduce the danger of foreign employees' desertion in the face of security threats by promoting programs to train local experts in their stead. The case of Nigeria shows that the oil companies' main concern is their foreign employees (engineers, managers, and technicians, who generally come from the West), while the local employees tend to continue to function even during emergencies. In order to ensure the facilities' operation during war or other security crises, Israel must promote professional training for Israeli personnel in energy and gas engineering. Such experts could gradually replace the foreign employees and therefore alleviate some of the concerns regarding the cost-effective nature of increased insurance and security. Though there is a cost involved in training local experts, it may be less expensive than that incurred by interrupting manufacturing processes in the event of a national crisis.

Efforts in this direction are already being made by the Israeli Ministry of National Infrastructures, Energy, and Water Resources. For the past three years, the ministry has been promoting a scholarship fund for students pursuing a bachelor's, master's, or PhD degree in engineering, physics, geology, and seismology in order to train manpower in energy-related fields.[25] However, this fund is limited in scope, and so far there are only a few dozen scholarship recipients. In order to attain more ambitious goals and allocate larger budgets for training local engineers and employees in the natural gas industry (with a specific emphasis on the low-tech professions connected to this industry), training a local workforce should be made a national strategic priority as part of Israel's efforts to ensure its energy security in the coming years.

Conclusion

The defense establishment in Israel places an emphasis on the need to physically protect Israeli gas installations against terrorist threats. The case of Nigeria demonstrates that ensuring the protection of the human infrastructure needed to operate these installations is no less important and can provide a long-term (and more cost efficient) solution to some of these threats. The case of Nigeria also indicates that when dealing with infrastructure that is critical to the economy, it is the state that is responsible for the safety of the employees operating it, even when these employees are foreigners who only operate in the state's exclusive economic zone, since it is the state that suffers should they abandon their work.

In the long run, true energy security can only be achieved by developing local expertise. This can be done by training Israeli personnel in the fields relevant to the industry (energy and gas engineering, physics and geology, and low-tech professions) who can be used even in emergencies and under fire. In a more optimistic scenario, other long-term solutions could include sharing reserves by exporting gas to Israel's neighbors (Jordan, Egypt, and the Palestinian Authority) or sharing exploration licenses in maritime conflict zones (the Israel-Lebanon border) in a manner that would transform the stability of production and export into a strategic interest for the entire region, and not just for Israel.

Notes

1 Amiram Barkat and Hillel Koren, "Woodside Buying 30% of Leviathan for $2.5b," *Globes*, December 3, 2012, http://www.globes.co.il/en/article-1000802994.

2 Yoaz Hendel, "Former Naval Commandos, Sayeret Matkal Soldiers, and Unit 669 Members Guard Noble Energy Drilling Rigs in Israel's Coastal Waters," *Globes*, February 26, 2009, http://www.mako.co.il/men-magazine/firepower/Article-fb0e254c92e9f11004.htm.

3 Noam Feig, "Potential Threats and Challenges in Protecting Maritime Energy Facilities," Conference on "Natural Gas Discoveries: Strategic Implications," Institute for National Security Studies, November 23, 2010, http://www.inss.org.il/heb/events.php?cat=293&incat=&read=4616. See also similar comments by Israel Navy commander General Ram Rotenberg in an interview with *Ha'aretz*: Amos Harel, "The Underprivileged Son in the General Staff Speaks Out," *Ha'aretz*, September 20, 2013.

4 Sherry Su, "Iraq Exports Less Kirkuk Crude from Ceyhan than Planned in 2013," *Bloomberg*, August 13, 2013, http://www.bloomberg.com/news/2013-08-13/iraq-exports-less-kirkuk-crude-from-ceyhan-than-planned-in-2013.html.

5 On the Iranian oil industry functioning during the Iran-Iraq War, see Farzin Nadimi, "Iran's Oil Industry at War and Some Lessons Learned for a Post-War Iran," in *Oil and War*, ed. Alain Beltran (Brussels: P.I.E. Peter Lang, 2012).

6 This principle is true mainly in Western oil and gas companies. It appears that Russian and Chinese energy companies are less sensitive to the possibility of harm to their employees during operations in a foreign country.

7 Comments by the Prime Minister on the State Comptroller's Report 58a, Prime Minister's Office, Senior Division, State and Internal Auditing, 2008, http://www.pmo.gov.il/NR/rdonlyres/40594B6D-61E1-4809-839B-78A4818817E2/0/report58bword.doc.

8 This comparison becomes even clearer when we take into account that shipping in Israel involves many foreign companies, which theoretically could compensate for each other if one should discontinue its operations in Israel (though not to a satisfactory level). The gas economy, on the other hand, is expected to involve only a few foreign companies, which would be difficult to quickly replace in the event of a breach of contract.

9 Figures on the Nigerian energy economy can be found on the US Energy Information Administration (EIA) website, http://www.eia.gov/countries/cab.cfm?fips=NI.

10 Eric Watkins, "Oil Worker Kidnappings Continue in Nigeria," *Oil & Gas Journal*, May 25, 2007, http://www.ogj.com/articles/2007/05/oil-worker-kidnappings-continue-in-nigeria.html.

11 Daniel Howden, "Nigeria: Shell May Pull Out of Niger Delta after 17 Die in Boat Raid," *Independent*, January 17, 2006, http://www.independent.co.uk/news/world/africa/shell-may-pull-out-of-niger-delta-after-17-die-in-boat-raid-523341.html.

12 Elias Courson, "MEND: Political Marginalization, Repression and Petro-Insurgency in the Niger Delta," *African Security*, 4, no. 1 (2011): 20-43.

13 Kimberly L. Jones, "Effect of Oil Terrorism on the Global Economy: A Case Study of Nigeria," *ASBBS eJournal*, 8, no. 1 (Summer 2012): 62-74, http://www.asbbs.org/files/2012/eJournal_2012.pdf.

14 Daniel Yergin, *The Quest: Energy, Security and the Remaking of the Modern World* (New York: Penguin Books, 2011), p. 137.

15 For tables illustrating the fluctuations in the pace of oil and gas production in Nigeria, see http://www.eia.gov/countries/cab.cfm?fips=NI.

16 Ben Amunwa, "Fuelling the Violence: Oil Companies and Armed Militancy in Nigeria," *Platform*, August 2012, http://platformlondon.org/wp-content/uploads/2012/08/Fuelling-the-violence-Oil-Companies-and-Armed-Militancy-in-Nigeria-August-2012.pdf.

17 Drew Hinshaw, "Nigeria's Former Oil Bandits Now Collect Government Cash," *Wall Street Journal*, August 22, 2012, http://online.wsj.com/article/SB10001424052702304019404577420160886588518.html.

18 David Smith, "Shell Accused of Fuelling Violence in Nigeria by Paying Rival Militant Gangs," *Guardian*, October 3, 2011, http://www.guardian.co.uk/world/2011/oct/03/shell-accused-of-fuelling-nigeria-conflict .

19 Guy Katzovitch, "Gas Fields Will Lead to Conflict in the Middle East: Hizbollah Liable to Attack," *Globes*, May 22, 2012, http://www.globes.co.il/news/article.aspx?did=1000750836.

20 Doron Peskin, "Hizbollah Official: We Will Not Allow Israel to Steal Lebanese Gas," June 14, 2010, http://www.calcalist.co.il/world/articles/0,7340,L-3407983,00.html.

21 These figures come from Woodside Petroleum's website, http://www.woodside.com.au/Our-Business/International/Pages/default.aspx.

22 These figures come from Noble Energy's website, http://www.nobleenergyinc.com/Operations/Overview-51.htm.

23 Seeing as Shell, which operated in Nigeria, has a 25 percent stake in Woodside Petroleum, it is not inconceivable that a solution involving payment of protection money will come up in a discussion of the company's preferences for its operations in Israel. In addition, Woodside Petroleum had come under scrutiny in regards to its operations in Mauritania exactly for these reasons.

24 On the potential for Israeli gas exports to neighboring Middle Eastern countries see Brenda Shaffer, "Israel – New Natural Gas Producer in the Mediterranean," *Energy Policy*, 39, no. 9 (2011): 5379-5387.

25 Press Release, "Undecided about What to Study? The Government Will Help You!" Ministry of National Infrastructures, Energy, and Water Resources website, June 24, 2012.

Sri Lanka and the Tamil Tigers: Conflict and Legitimacy

Shlomi Yass

The Liberation Tigers of Tamil Eelam (LTTE) was founded in 1976, demanding the establishment of an independent state for the Tamil ethnic minority in northern and northeastern Sri Lanka. In May 2009, following over three decades of conflict, its leader, Velupillai Prabhakaran was killed and the group was dismantled. The LTTE was established long before other well-known terror groups emerged, and yet it received little attention in comparison. An analysis of the relations between Sri Lankan governments and the Tamil Tigers from the onset of the struggle in the 1970s up to the group's final defeat in May 2009 can provide valuable lessons to other democratic states fighting terrorist organizations, including Israel.

Keywords: Sri Lanka, Tamil Tigers, terrorist organizations, Sinhalese, Tamils, legitimacy, negotiations, conflict, Israeli-Palestinian conflict, Israel

The terrorist organization known as the Liberation Tigers of Tamil Eelam (LTTE) was founded in 1976, demanding the establishment of an independent Tamil state in northern and northeastern Sri Lanka. In May 2009, following over three decades of conflict, its leader, Velupillai Prabhakaran was killed and the group was dismantled.

Upon its establishment, the LTTE had supported a Marxist-Leninist ideology. In addition, it called for recognition of the Hindu religion and Tamil language in the country and for appropriate representation in the universities, employment, and the public sector. These demands evolved into a separatist nationalist ideology, as the LTTE demanded an independent Tamil state.

Shlomi Yass is an intern in the Military and Strategic Affairs Program at the Institute for National Security Studies.

The profile of the Tamil Tigers differs from that of other terrorist groups. It did not seek liberation from a foreign occupier, and its ideology was secular. The LTTE operated a navy, an air force, a women's brigade, an orphaned children's brigade, an elite suicide force, and a cyberwarfare unit, long before other well-known terrorist groups employed such measures.

The last Sri Lankan president to face the LTTE, Mahinda Rajapaksa, was able to adopt a drastic policy of all-out war against the organization due to an atmosphere of ongoing violence, failed rounds of negotiations, and a heavy toll on the economy. This atmosphere, along with the general sentiment of a global war on terror created in the aftermath of September 11, 2001, facilitated extreme action such as imposing censorship on Tamil media and utilizing pro-government media in delegitimizing the LTTE, and towards the end of the conflict the government denied the UN, foreign media, and human rights organizations access to the battle zones. A sharp increase in weapons' acquisition from foreign countries, primarily Israel, provided the Sri Lankan government with the operative edge needed to completely defeat the organization in 2009.

An analysis of the relations between Sri Lankan governments and the LTTE throughout the years can serve as a valuable source of information and lessons for the international community in its fight against terror.

Sri Lanka and the Tamil Tigers: A History of the Conflict

Originally known as Ceylon ("the Holy Island"), Sri Lanka is located near the southeastern coast of the Indian subcontinent, in the Indian Ocean. Its population of 21 million resides in an area of about 65,600 square kilometers. The Sinhalese ("lions") are the largest ethnic group, constituting 73.8 percent of the population, while the Tamils ("tigers") constitute 12 percent, and the descendants of the Arab traders ("Moors") constitute 9 percent. The main religions are Buddhism, Hinduism, and Islam, respectively.[1]

In the sixteenth and seventeenth centuries, the Portuguese and Dutch controlled the island. In the eighteenth century it became a British colony, and hundreds of thousands of ethnic Tamils were brought by the British from southern India to work in the tea, coffee, and coconut plantations. The origin of the struggle between the two dominant ethnic groups, the Sinhalese and the Tamils, can be traced back to the British policy of "divide and conquer." Despite their numerical inferiority, under the British the Tamils held a disproportionate number of positions in the public service and were over-represented in government institutions.

In 1948, the island became a British Commonwealth Dominion, with independent control over foreign relations and defense. The Sinhalese majority sought to assert its religion, its language, and its culture on the entire country at the expense of the Tamil minority. The Ceylon Citizenship Act was passed, denying citizenship to the Tamil plantation workers who had come from India. As a result, the Tamils began promoting the establishment of a federal system with a Tamil autonomy.[2]

In 1956, Solomon Bandaranaike, a Sinhalese, was elected Prime Minister. The Sinhala Exclusivity Act was passed, establishing Sinhalese as the official language and limiting the number of Tamil employees in the public service.[3] In 1957 and 1965, agreements were signed discussing the status of the Tamil language and decentralization of part of the political power through its transfer to the provincial councils, but neither was honored because of Sinhalese objection within the government.

In 1972, the island received independence from Great Britain and changed its name from Ceylon to Sri Lanka. The new constitution continued the policy of discrimination, making Buddhism the dominant religion in the country and establishing restrictions on the number of Tamils attending universities.[4] As a result, many Tamil communities began migrating to the northern and northeastern parts of the country.

Although at a certain point more than forty-two official Tamil groups operated in Sri Lanka, there was no meaningful Tamil representation in the political system. This vacuum was quickly filled by armed groups. In 1976, an unknown eighteen-year-old by the name of Velupillai Prabhakara established the Liberation Tigers of Tamil Eelam (LTTE). His charismatic and dictatorial leadership style allowed him to lead the organization for over three decades.

In 1981, the Sinhalese took to the streets in a violent campaign against the Tamil minority and set fire to the Tamil public library in Jaffna. The library held over 100,000 rare ancient manuscripts and was considered the main Tamil cultural institution.[5] Two years later, riots broke out in what was later termed "Black July," following the killing of thirteen Sinhalese soldiers by Tamil rebels. For several days, a retaliation campaign was carried out, during which masses of Sinhalese, with the aid of the army, raided Tamil homes, looted their property, and killed thousands. The "Black July" riots led hundreds of thousands of Tamils to flee the country and marked a watershed in the civil war between the Sinhalese and the Tamils.[6]

At the time, following pressure from its Tamil citizens in the state of Tamil Nadu, India offered support in negotiations between the rival groups.[7] It assisted in establishing training camps in Indian territory and later sent its "peace force" to oversee implementation of local ceasefire agreements. It was not long before the Indians were dragged into military involvement by Tamil rebels. The "peace force" did have some success, but it lost over 1,500 soldiers.[8] In light of these losses, criticism at home, and the elections in India and Sri Lanka, India retreated from its peace initiative in 1990.

The lack of external intervention allowed the LTTE to establish its position as the dominant Tamil organization, and the suicide attacks against military targets expanded to assassinations of politicians and civilians.[9] Upon its establishment, the LTTE formed ties with the Palestine Liberation Organization (PLO) in London, including training of Tamil rebels in Middle Eastern refugee camps.[10] The relationship expanded and later included Hamas, Hizbollah, and the Popular Front for the Liberation of Palestine, headed by George Habash.[11] In 1990, the Tamil Tigers attacked a Sri Lanka military base using chlorine gas, wounding more than sixty soldiers,[12] and a year later, the group carried out a naval suicide attack against a Sri Lankan supply ship.[13] In 1991, a female suicide bomber assassinated former Indian Prime Minister Rajiv Gandhi Premadasa on Sri Lankan soil, and in 1993, Sri Lankan President Ranasinghe Premadasa was killed in a suicide attack. In 1997, the world's first cyber attack was carried out against Sri Lankan embassies around the globe, as over 800 e-mails a day flooded the embassies and paralyzed embassy networks for almost two weeks (figure 1).[14] Through the LTTE, stolen Norwegian passports made their way to al-Qaeda in 1993 and reached operatives such as Ramzi Yousef, one of the planners of the attack on the World Trade Center.[15] It is possible that Tamil rebel merchant ships were used to transfer weapons to al-Qaeda as well.[16]

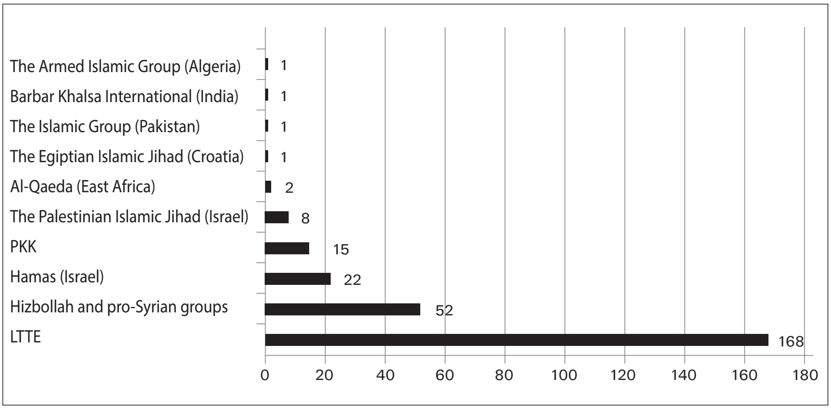


Figure 1. Suicide Attacks Carried out by Various Groups (1980-2000)
Source: Gunaratna (2000)

In 1990, the Tamil Tigers began to expel tens of thousands of Muslims from the areas under their control in northern Sri Lanka and reinforced their military and civilian control in the north, particularly the Jaffna district. Up to the year 2000, a de facto state called Tamil Eelam governed the northern provinces, with a flag and a national anthem, a court, a police force, and even a taxation system, alongside the official Sri Lankan system.[17]

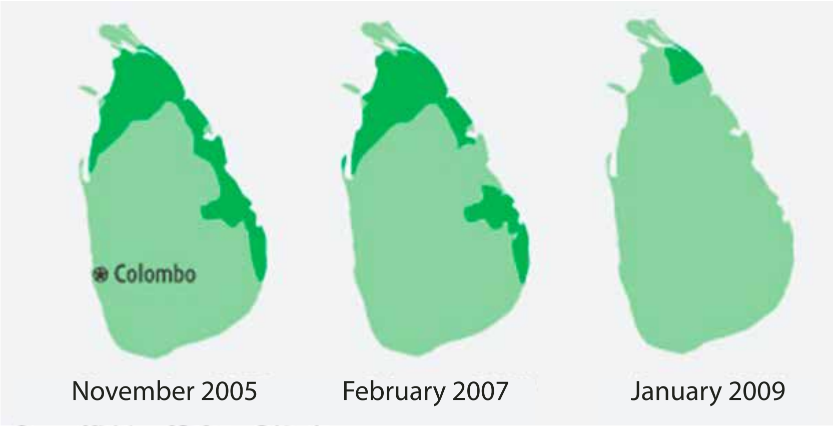
In 1999, Norway—which was considered a neutral country with no colonialist past or hidden political and economic agendas—began to assist in the negotiations. Norway's involvement in negotiations for the Oslo Accords between Israel and the PLO had made it a favorable mediator. Two years later, the Tamil Tigers declared a unilateral ceasefire, and a short time after that, a joint memorandum of understanding was signed. Under Norwegian auspices, six meetings were held, but repeated violations on behalf of Sri Lanka led the LTTE to announce in 2003 that the talks were suspended.

The Tamil Tigers' Defeat

In 2005, Mahinda Rajapakse was elected president of Sri Lanka and continued the attempted dialogue with the LTTE. As a result of the continuing suicide attacks and military raids, in 2008 the government in Colombo abandoned its attempts to achieve a ceasefire and decided to strive tawards a military strike.[18]

The operation aimed at defeating the Tamil rebels took place between January and May 2009. In January, the Tamil Tigers' capital, the city of Kilinochchi in the north of the island, was captured. The media, United Nations, and human rights organizations were denied access, and websites affiliated with the LTTE were blocked (TamilNet being the most prominent). A rebel force defending the city withdrew to the jungles along with hundreds of thousands of trapped civilians serving as human shields (figure 2). As a result of heavy pressure from the international community, the government established no-fire zones, calling upon civilians to move to these areas. Shortly after, the army bombed these areas, ignoring the UN and human rights organizations' pleas. In April, the rebels' defensive line was breached, creating a corridor through which civilians were able to flee from their rebel captors.[19] On May 16, the army gained control of the last rebel strongholds, and two days later, Velupillai Prabhakaran was killed and thirty years of civil war came to an end.

Losing Ground



🟩 Approximate Tamil Tiger areas

Figure 2. Tamil Tiger-controlled areas 2005-2009
Source: Ministry of Defense, Sri Lanka

The Victims of the Conflict

Between 1972 and 2009, at least 100,000 people were killed in Sri Lanka, 40,000 of them in the last months of fighting.[20] The UN rejected claims by the government that during these last months it undertook a "humanitarian rescue operation" with a policy of "zero civilian casualties."[21] It was the UN's recommendation to commence international investigation on account of suspected human rights violations, war crimes, and crimes against humanity.

Recently, the government admitted that in the last months of fighting, 9,000 people were killed.[22] However, the Northern Provincial Council, the Tamil council in the north of Sri Lanka, announced that it does not accept this government statistic because it is "flawed," and it carried out its own investigation.[23] The fierce worldwide debate regarding both sides' conduct, especially in the last months of the fighting, is far from over and will continue for a long time.

The Issue of the Definition of Terrorism

The case of Sri Lanka and the Tamil Tigers is a classic example of the problematic nature of the term "terrorism." Although the term is used often, it has no universally accepted definition, and in fact, there are hundreds of definitions. Not infrequently, the definitions are a result of political considerations and narrow interests rather than a true joint effort to establish a coherent definition. The lack of definition is not merely an academic issue. In practice, it interferes with setting uniform standards and leads to a blurring between areas of responsibility, preventative measures, legal aspects, and the like.[24]

Legitimacy

Every regime's stability is dependent upon its degree of legitimacy. Although many people use the term "legitimacy," few define it. Legitimacy is in the eyes of the beholder, it is a belief and a subjective mindset. As such, it includes a broad range of interpretations: moral, ethical, legal, and others. In general, one can say that legitimacy is a process by means of which an entity is able to justify its existence.[25]

The idea of legitimacy is associated with the German sociologist Max Weber, who emphasized three types of authority: traditional authority, emanating from belief or tradition and based on the laws of inheritance; charismatic authority, relying on an exceptional leader whose mission and vision are an inspiration to others; and legal-rational authority, which is based on laws and normative regulations,[26] and which is customary in democratic regimes.

Political legitimacy is the recognition of the right to govern. This is achieved through the belief that the political institutions are the most appropriate for a specific society. The regime's legitimacy relies on the populace's adherence, law enforcement, and society's accepted norms.[27] Legitimacy can also be defined by its absence. An example is the campaign to delegitimize Israel and the denial of the Jewish people's right to self-determination through the State of Israel.[28]

The events of September 11, 2001 catalyzed a global change in the attitude toward terror organizations. The real-time feed from the scene shocked the international community. As a result, the battle waged by states against terror organizations achieved greater legitimacy than in the past.

Sri Lanka was able to aptly exploit the global change in attitude towards terror, targeting the LTTE through controversial military methods, alongside an aggressive and organized media campaign to mobilize domestic and international public opinion. These vigorous, ongoing measures led to the erosion of the LTTE's legitimacy, and consequently, despite the world's condemnations and the clear evidence that both parties were carrying out war crimes and crimes against humanity, especially in the last months of the fighting in 2009, Sri Lanka was never labeled a terrorist state.

Who is a Terrorist?

If Sri Lanka was not a terrorist state, then why were the Tamil Tigers terrorists? In the September 11 aftermath, as well as the attacks in Bali in 2002, in Madrid in 2004, in London in 2005, and many others, an increasing number of countries became affected by terror, forcing them to take a stand against those who perpetrated the attacks. World public opinion was no longer in favor of the LTTE, no matter how justified its objective, as it used female fighters and recruited orphaned children. Furthermore, the organization's international network, which included fifty-four Tamil organizations and was the source of its economic, political, and propaganda capabilities, lost its power. This was accompanied by significant criticism from Tamil citizens, and certainly Sinhalese citizens in Sri Lanka itself, on account of the assassination of numerous politicians, government officials, academics, and intellectuals.

The LTTE's legitimacy in the domestic and international arena was eroded. Indeed, by 2006, no fewer than thirty-two countries had placed the Tamil

Tigers on their list of terrorist organizations, among them India, Canada, the European Union, the United States, Great Britain, and Sri Lanka.[29]

Israeli Involvement

Relations between Sri Lanka and Israel have ebbed and flowed since the establishment of diplomatic relations between the countries in 1956. Sri Lanka broke off relations on a number of occasions, mainly as a result of pressure from the Arab world and opposition by the country's Muslim population. Later, in light of the ongoing conflict against the Tamil rebels, it sought Israel's help in a number of areas, particularly security.[30]

Many countries have provided Sri Lanka with weapons, including the Ukraine, Iran, Russia, Pakistan, China, England, and the United States.[31] However, Israel stands out in regards to the scope of weapons provided, reaching hundreds of millions of USD (figure 3). The Sri Lankan army purchased advanced night vision and communications technology, artillery-coordination systems, and Gabriel sea-to-sea missiles. In addition, it acquired drones and ground stations, flak jackets, ammunition, thousands of Uzi submachine guns and Galil assault weapons, mortars, and 155-mm cannons.[32]

A special emphasis was placed on acquiring weapons for the Sri Lankan Navy and Air Force. As early as the 1950s, the Sri Lankan navy purchased the Israeli Miznak and Mivtach naval vessels. Later it acquired the Sa'ar, the Shaldag, the Dvora, and the Super Dvora.[33] By increasing its operational range through Israeli vessels, the Sri Lankan navy was able to effectively fight the Tamil Tigers' naval force, as the Tamils used the sea as the main channel for smuggling weapons and operatives from India, attacking the Sri Lankan navy and even sinking six Sri Lankan Dvora-class boats.[34]

As for the Sri Lankan air force, in 1995 it purchased seven Kfir Fighter Jets, and in 2000, it was reported that eight more jets had been purchased. The Israeli jets played a pivotal role: one of the Kfir squadrons logged more than 2,800 operational flight hours and released over 3,500 tons of bombs.[35] The Sri Lankan ambassador to Israel confirmed that pilots from his country had received training in Israel,[36] and a spokesman for the Sri Lankan embassy in Washington even stated that Israeli pilots had actually flown the planes.[37]

Furthermore, there were reports that Israeli submarines carried out test launches of Popeye missiles, which are capable of carrying a nuclear warhead, near Sri Lanka's coast in the Indian Ocean.[38] Israel had record arms sales, more than any other country in the world in the past twenty years.[39] There is no doubt that the Israeli weapons and vessels provided Sri Lanka with an operative edge; the jets and boats allowed the military to strike the Tamil rebels from a greater distance, thereby challenging the Tamil forces.

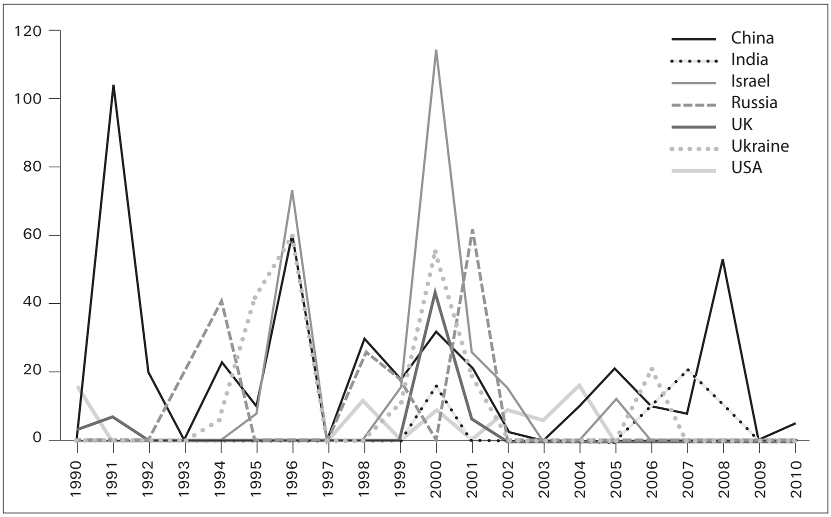


Figure 3. Supply of Weapons to Sri Lanka
Source: Stockholm International Peace Research Institute: (SIPRI), Arms Transfers Database.

Iranian Involvement

The budding relations between Sri Lanka and Iran have put a halt to the military collaboration between Israel and Sri Lanka. During 2008, Sri Lankan president Mahinda Rajapaksa and Iranian president Mahmoud Ahmadinejad held a number of meetings, during which several agreements were signed. Iran pledged 1.9 billion dollars in soft loans and grants in order to develop irrigation and hydroelectric power projects, while Sri Lanka pledged to purchase Iranian oil.[40]

Another meeting took place recently between President Rajapaksa and Iranian president Hassan Rouhani, indicating that ties between the two countries are strengthening. At the meeting, the two leaders discussed the need to explore possibilities for increasing bilateral trade in goods and services.[41]

The new alliance and resulting danger that Israeli technology may fall in the hands of Tehran, caused Israel to freeze defense exports to Sri Lanka, despite the extension of bilateral relations in trade, agriculture, irrigation, and desalination.[42]

The Connection between the Conflict in Sri Lanka and the Israeli-Palestinian Conflict

Though other terrorist organizations may share similar features, the LTTE differs from contemporary terrorist organizations in several ways. Similarities include the absence of negotiations, the use of suicide bombers and sources of funding.

The absence of negotiations: the negotiations between the LTTE and Sri Lanka were few and far apart, suffering from long periods of stalemate, complete lack of trust, and mutual breaches. Indian and Norwegian attempts to mediate deliberations led to a temporary cessation of the violence.

The Israeli-Palestinian conflict is characterized by ongoing fighting with repeated attempts to "revive" or "jumpstart" the "moribund" negotiations. This conflict also suffers from lack of trust, stalemate and breaches of agreements.

The use of suicide bombers: initially, the LTTE was in search of its own distinct niche in a field already laden with competing militant organizations. As a non-state actor fighting a globally recognized political entity, the LTTE turned to suicide bombers in order to achieve an operational edge and distinguish itself from other actors. Hamas, like the Tamil Tigers, created a distinctive niche through the use of suicide bombers.[43]

Hamas's challenge, however, was more difficult. As a latecomer to an arena that already had a well-established Palestinian liberation movement, Hamas had to distinguish itself from competing terrorist organizations, as well as the PLO.

Sources of funding: terrorist organizations require funding in order to realize their objectives. Such funding can emanate from the general public, self-financing, ostensibly legitimate businesses, illegal activities, and terror-supporting states. The events of September 11 emphasized the pivotal role of funding in maintaining a terrorist organization.

The Tamil Tigers financed their operations though fundraising and extensive criminal activity. The Tamil diaspora operated dozens of organizations around the world,[44] and at least thirty-two front companies disguised as charitable organizations. The criminal activity included maritime piracy, human, drug and weapons smuggling, threats, extortion, and passport and credit card forgery. It is estimated that the Tamil Tigers accumulated between 200 and 300 million dollars annually from legal and illegal businesses.[45]

The Palestinian terrorist organizations, like the Tamil Tigers, are funded not only by foundations and contributions from private institutions, but also state actors such as Saudi Arabia, Iran, and Syria.[46] A significant proportion of financial support emanates from Iran, estimated at tens of millions of dollars every month,[47] and from Hizbollah, which launders large sums of money in Lebanon. The Islamic Jihad in Palestine receives most of its funding from Iran, while Hizbollah provides training bases and logistical aid.[48]

The following are areas in which the Tamil Tigers and Palestinian terrorist organizations operating against Israel differ.

Lack of recognition: both conflicts included a territorial claim. However, the Tamil Tigers recognized Sri Lanka's independence and the Sinhalese majority's legitimacy to exist in the country, though they demanded the establishment of an independent Tamil state alongside the independent Sinhalese state. In contrast, Hamas and the Palestinian Islamic Jihad are expressly anti-Western organizations that have frequently called for the destruction of the State of Israel and they continue to refuse to recognize its right to exist.

Multiple organizations: though at the onset of the struggle there were dozens of militant Tamil organizations, they very quickly dissipated. Whether due to lack of an ideological platform or because operatives moved to other organizations or were killed, as of the 1990s, the Tamil Tigers became the sole representatives of the Tamils in Sri Lanka. In contrast, in the Israeli-Palestinian conflict, there are many organizations with different and often contradictory characteristics and objectives.

Ideological flexibility: The Tamil Tigers took a forceful, unequivocal approach throughout their years of existence: an uncompromising demand for an independent state in northern Sri Lanka. Although the group's methods of operation became increasingly sophisticated over the years, its ideological platform was conservative and its nationalist objective was very basic. In contrast, the ideological platform of some of the Palestinian organizations has shifted over time: If in the beginning, all Palestinian factions supported terror in order to obtain political rights, in recent years there has been a change, at least on the declarative level, with the PLO, the Palestinian umbrella organization, repeatedly stating that the path of terror has failed and that the rights of the Palestinian people will be restored only through the use of diplomacy.

Media coverage: The Tamil Tigers were one of the most deadly terror organizations in the modern period. However, the conflict in Sri Lanka received less media coverage than other conflicts, such as the Israeli-Palestinian conflict, because of the Western tradition of "mental distance" from events taking place in Asian countries—a lack of sufficient attention, to the point of intentional disregard. In the first months of 2009, the average daily headline coverage of the two conflicts around the world was clearly unbalanced: the Sri Lankan conflict received an average of 29 headlines a day, while the Israeli-Palestinian conflict received an average of 148 a day.[49]

Conclusions and Recommendations

The conflict in Sri Lanka provides insight into the characteristics shared with the Israeli-Palestinian conflict. Nevertheless, there are three main issues that should be noted: time as an element of the conflict, placing terrorist groups on a list of terrorist organizations, and expanding involvement.

Time as an element of the conflict: a prolonged conflict does not exist in a vacuum. It facilitates entrenchment and a stalemate.

There is no doubt that in Sri Lanka, the lack of a true ceasefire, along with the prolonged stalemate, were harmful for both sides. As the years passed without a permanent agreement, or at least a significant respite in the fighting, an additional critical, negative dimension was added: the element of time. The feelings of hostility and alienation intensified the already common prejudices between the sides. The Tamil protest, which, like the government response, was at first mainly non-violent, deteriorated into systematic organized violence, while the government responded by killing thousands.

As for the Israeli-Palestinian conflict, it would be an error to assume that maintaining the status quo between Israel and the Palestinians is preferable to an agreement that includes concessions. An example of this can be found in the evolution reflected in Hamas's appearance as a counterweight to the PLO, and years later, in the flood of extremist entities emerging as a counterweight to Hamas. Another dangerous example, which is gaining momentum, is the rise in attacks initiated by Israeli settlers against Palestinians, referred to in politically correct language as "price tag" attacks. These acts clearly demonstrate the change that has taken place in Israel over the years as a result of the failed negotiations. The U.S. State Department's latest report on global terror places settlers in the same position as terror organizations, and there is a worrying increase in the number of attacks reported in the previous year.[50] What will happen with the Israeli-Palestinian conflict (and the conflict between Israel and the Arab world) if such actions spin out of control?

Placing terror groups on a list of terrorist organizations: it is extremely important to promote listing terrorist organizations as such, supporting the notion that a war over the legitimacy of a terrorist organization is preferable to a war against it on the battlefield.

Sri Lanka did a good job of damaging the legitimacy of the Tamil Tigers, inter alia, by working actively and effectively to have the group placed on the list of terrorist organizations. Not only was benefit derived from providing a counterweight to international Tamil propaganda and damage caused to the Tamil narrative, but global cooperation against the organization expanded. These aggressive actions limited the group's maneuvering capabilities in the legal arena, significantly hindering its sources of funding, and decisively contributing to damaging its legitimacy.

Israel, too, must work intensively—beyond prevention and punishment, beyond targeting sources of funding and limiting maneuvering room—to increase cooperation and to create a common fate with other countries and their agencies, institutions, and organizations. It should conduct an effective international information campaign that includes countries both near and far, make use of coordinated diplomacy, and take a clear stand against countries that support terrorist organizations, whether directly or indirectly. These all should be done with a clear intention to increase the circle of states that place Palestinian terrorist groups on a list of terrorist organizations.

Expanding involvement: Even though a partnership with additional actors in the frameworks of negotiations makes concessions necessary, when a solution is found, such a partnership will enable a more comprehensive and stable agreement.

The Tamil Tigers were a narrow secular nationalist group in terms of ideology and territory. Nevertheless, because of the long tradition of religious tension between the Sinhalese majority, who are Buddhists, and the Tamil minority, who are Hindus, it is not inconceivable that the ethnic issue in the conflict was only one layer, perhaps a marginal one, compared to the religious issue.

As for the Israeli-Palestinian conflict, the two main groups, Hamas and the Islamic Jihad in Palestine, are fundamentally religious organizations. In Hamas's opinion, the "problem of Palestine" is a Muslim religious problem, and the territory of "Palestine" is Muslim holy land, and thus giving up even one inch of it is strictly prohibited.[51] The Islamic Jihad in Palestine also claims that the Palestinian problem is not national, but fundamentally Islamic, and that solving it is the key to liberating and uniting the entire Muslim nation.[52]

Since the Israeli-Palestinian conflict involves a broad religious problem, extending well beyond the narrow nationalist issue, it would be desirable to give weight to positive, moderate forces. This includes giving serious consideration to extensive involvement by the Arab states. The Arab peace initiative, with the necessary changes, could be a good starting point.

Notes

[1] CIA, "Sri Lanka," April 21, 2014, *The World Factbook*, https://www.cia.gov/library/publications/the-world-factbook/geos/ce.html.

[2] "Timeline: History of the Conflict in Sri Lanka," PBS, June 27, 2006, http://www.pbs.org/pov/nomoretears/special_timeline.php.

[3] V. P. Vaidik, *Ethnic Crisis in Sri Lanka: India's Options* (South Asia Books, 1986), p. 75.

[4] "Sri Lanka: Country Overview," *Encyclopedia of the Nations*, 2013, http://www.nationsencyclopedia.com/economies/Asia-and-the-Pacific/Sri-Lanka.html.

[5] Rebecca Knuth, "Destroying a Symbol: Checkered History of Sri Lanka's Jaffna Public Library" in *72nd IFLA General Conference and Council, 20-24 August, 2006*. http://tamilnation.co/indictment/rebecca.pdf.

[6] Frances Harrison, "Twenty Years On – Riots That Led to War," *BBC*, July 23, 2003, http://news.bbc.co.uk/2/hi/south_asia/3090111.stm.

[7] Australian Government, Department of Foreign Affairs and Trade. *Sri Lanka Country Brief* 2012, http://www.dfat.gov.au/geo/sri_lanka/sri_lanka_country_brief.html.

[8] “Peace That the LTTE Spurned,” *Sunday Times*, May 24, 2009, http://www.sundaytimes.lk/090524/News/sundaytimesnews_28.html.

[9] European Center for Constitutional and Human Rights, *Study on Criminal Accountability in Sri Lanka as of January 2009*, June 2010.

[10] S.V.D Gamini Samarnayake, *Political Violence in Sri Lanka 1971-1987* (New Delhi: Gyan Publishing House, 2008), p. 233.

[11] Bharat Verma, *Indian Defence Review* (New Delhi: Lancer Publishers, 2010), p. 107.

[12] John Parachini, “Putting WMD Terrorism into Perspective,” *Project MUSE* (2011), http://faculty.maxwell.syr.edu/rdenever/PPA%20730-11/Parachini.pdf, p. 39.

[13] Gunaratna, Dr Rohan. “The Threat to the Maritime Domain: How Real Is the Terrorist Threat?” *William B. Ruger Chair of National Security Economics Papers,* found at *http://www. nwc. navy. mil/nsdm/Rugerpapers. htm* (2008), p. 25.

[14] "Liberation Tigers of Tamil Eelam (LTTE): Internet Black Tigers,” Start, 2013, http://www.start.umd.edu/start/data_collections/tops/terrorist_organization_profile.asp?id=4062.

[15] Walter Jayawardhana, “LTTE Supplied Forged Passport to WTC Killer Ramzi Yousef,” *Ministry of Defence and Urban Development*, December 30, 2010, http://www.defence.lk/new.asp?fname=20070324_03.

[16] “Possible Links between LTTE and al-Qaeda,” *The Sunday Times*, February 4, 2007, http://www.sundaytimes.lk/070204/News/105news.html.

[17] “Peace Negotiations of Sri Lankan Conflict in 2000-2006 (2007), http://www.diva-portal.org/smash/get/diva2:4488/FULLTEXT01.pdf, p. 17.

[18] From an interview with Donald Perera, Sri Lanka’s ambassador to Israel, at the ambassador’s residence in Tel Aviv, September 21, 2011.

[19] Jon Lee Anderson, “Death of the Tiger,” Ilankai Tamil Sangam (2011), http://www.sangam.org/2011/01/Death_of_the_Tiger.pdf, p. 42.

[20] “UN Seeks Foreign Probe of Sri Lanka War Crimes,” *ABC*, February 16, 2014, http://www.abc.net.au/news/2014-02-16/an-un-seeks-foreign-probe-of-sri-lanka-war-crimes/5263122.

[21] “Report of the Secretary-General’s Panel of Experts on Accountability in Sri Lanka,” *UN,* March 31, 2011, , http://www.un.org/News/dh/infocus/Sri_Lanka/POE_Report_Full.pdf. p. 10.

[22] Charles Haviland, “Sri Lanka Government Publishes War Death Toll Statistics,” BBC, February 24, 2012, http://www.bbc.com/news/world-asia-17156686.

[23] “Tamil Council to Count Sri Lanka War Casualties,” *Arab News*, December 26, 2013, http://www.arabnews.com/news/498801.

[24] Martha Crenshaw, “The Psychology of Terrorism: An Agenda for the 21st Century,” *Political Psychology* 21, no. 2 (2000): p. 406.

[25] Mark C. Suchman, “Managing Legitimacy: Strategic and Institutional Approaches,” *Academy of Management Review* 20, no. 3 (1995): 572.

26 Max Weber. "The Three Types of Legitimate Rule," *Berkeley Publications in Society and Institutions* 4, no. 1 (1958): 1-11.

27 Jean-Marc Coicaud, *Legitimacy and Politics: A Contribution to the Study of Political Right and Political Responsibility* (Cambridge: Cambridge University Press, 2002), pp. 10-14.

28 "Basic Delegitimization for Israel," *Reut Institute*, July 2, 2004, http://www.reut-institute.org/he/Publication.aspx?PublicationId=285.

29 Amit Baruah, "European Union Bans LTTE," *The Hindu*, May 31, 2006, http://www.hindu.com/2006/05/31/stories/2006053117200100.htm.

30 Israel Ministry of Foreign Affairs, "Joint Communique regarding the Re-establishment of Diplomatic Ties between Israel and Sri Lanka," May 15, 2000, http://mfa.gov.il/MFA/ForeignPolicy/MFADocuments/Yearbook13/Pages/108%20%20Joint%20communiqu-eacute-%20regarding%20the%20re-esta.aspx.

31 "India and Sri Lanka after the LTTE," International Crisis Group, June 23, 2011, http://www.crisisgroup.org/en/regions/asia/south-asia/sri-lanka/206-india-and-sri-lanka-after-the-ltte.aspx.

32 Nadav Zeevi, "Defense Officials Fear Military Know-how Being Leaked to Iran," *Ma'ariv*, July 28, 2008, http://www.nrg.co.il/online/1/ART1/765/866.html.

33 "Ceylon (Sri Lanka)," Israeli Navy Veterans' Association web site, 2014.

34 "Sri Lanka Learns to Counter Sea Tigers' Swarm Tactics," *Jane's Navy International*, March 2009, http://www.defence.lk/news/Sri_Lanka_Navy.pdf.

35 David Eshel, "IAI Looks East to Sell Updated Kfirs," *Aviation Week*, Feb 3, 2014, http://aviationweek.com/awin/iai-looks-east-sell-updated-kfirs.

36 David Regev, "Sri Lankan Ambassador: We Back Israel's War on Terror," *Ynet*, July 2, 2010, http://www.ynetnews.com/articles/0,7340,L-3923309,00.html.

37 Jeffrey Phillips, "Tamil Secession Ruled Out," *BBC*, July 21, 2000, http://news.bbc.co.uk/2/hi/south_asia/844780.stm.

38 "Popeye Turbo," Federation of American Scientists, June 20, 2000, http://www.fas.org/nuke/guide/israel/missile/popeye-t.htm.

39 Katharine Tengtio, "International Dimensions of the Sri Lankan Conflict," Center for Peace & Conflict Studies (2013), http://www.academia.edu/3050746/International_Dimensions_of_the_Sri_Lankan_Conflict, p. 18.

40 "Iranian President Visits Sri Lanka," *USA Today*, April 28, 2008, http://usatoday30.usatoday.com/news/world/2008-04-28-iran-srilanka_N.htm.

41 "Lanka Wants Stronger Ties with Iran," *Colombo Gazette*, May 21, 2014, http://colombogazette.com/2014/05/21/lanka-wants-stronger-ties-with-iran.

42 "Sri Lanka and Israel Expand Bilateral Relations," *Daily News*, January 9, 2014, http://www.dailynews.lk/?q=local/sri-lanka-and-israel-expand-bilateral-relations.

43 Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2006), p. 135.

44 Brenda J. and James M. Lutz, *Global Terrorism* (Oxford: Routledge, 2008), p. 248.

45 Peter Mandaville and Terrence Lyons, *Politics from Afar: Transnational Diasporas and Networks* (New York: Columbia University Press, 2012), p. 102.

46 Felix Frisch, "Israel: Most Hamas Funding Coming from Saudi Arabia," *Ynet*, July 3, 2003, http://www.ynet.co.il/articles/1,7340,L-2710673,00.html.

47 Reuters, "Hamas: Our Relations with Iran Have Suffered; Iranians Sending Less Money," *Ynet*, June 3, 2013, http://www.ynet.co.il/articles/0,7340,L-4394563,00.html.

48 Lior Ben David, "Background Document on the Issue of Terrorist Organizations Fighting Israel," Knesset Research and Information Center, September 2, 2004, http://www.knesset.gov.il/mmm/data/pdf/m01048.pdf.

49 Noah Bernstein, "A Media Eclipse: Israel-Palestine and the World's Forgotten Conflicts," *Open Democracy*, March 18, 2010, http://www.opendemocracy.net/opensecurity/noah-bernstein/media-eclipse-israel-palestine-and-worlds-forgotten-conflicts.

50 Office of the Spokesperson, "Country Reports on Terrorism 2013," U.S. State Department, April 30, 2014, http://www.state.gov/r/pa/prs/ps/2014/04/225406.htm.

51 "The Hamas Charter (1988)," *Intelligence and Terrorism Information Center at the Center for Special Studies*, March 21, 2006, http://www.terrorism-info.org.il/data/pdf/PDF_06_032_2.pdf.

52 Lior Ben David, "Background Document on the Issue of Terrorist Organizations Fighting Israel," Knesset Research and Information Center, September 2, 2004, http://www.knesset.gov.il/mmm/data/pdf/m01048.pdf.

Developments in Iranian Cyber Warfare 2013-2014

Gabi Siboni and Sami Kronenfeld

In the course of 2013, Iran became one of the key players in the international cyber warfare theater. This development is a result of both defensive and offensive cyber force buildup processes and a measured relaxation of restraints on the part of Iranian decision makers with respect to offensive activity in cyberspace. Indeed, the Iranian activity points to major qualitative advances in Iran's technological and operational cyber capabilities. This article examines the activity and progress in Iran's cyber defense system, and the regime's use of this capability to restrain internal opposition. In addition, it looks at the offensive dimension, particularly cyber-attacks traced to Iranian agencies, agents, and allies.

Keywords: cyber, Iran, cyber security, cyber defense, networks isolation

Introduction

In an interview to the Atlantic Council, an American research institute, a senior source in the CrowdStrike Cyber Security Company rated Iran as a "third tier" country in regards to its cyberspace capabilities, stating that its cyber warfare capabilities were substantially inferior to those of "first tier" countries, such as the US, Russia, and the UK, as well as "second tier" countries such as China. This conception is in line with many Western intelligence specialists and administration officials. Iran is perceived as capable of harassing Western security systems and damaging "soft" targets, while lacking the knowledge and means to execute strategic cyber-attacks.[1] Nevertheless, during 2013, Iran became one of the key players in the international cyber warfare theater. It appears that this development is

Dr. Gabi Siboni is a senior research fellow and head of the INSS Cyber Warfare Program. Sami Kronenfeld is an intern in the Cyber Warfare Program at INSS.

a result of a combination of a measured relaxation of restraints on the part of Iranian decision makers with respect to offensive activity in cyberspace, and a major qualitative advance in the Iranian cyber warfare apparatus, which has surprised many Western experts in the extent of its activity, its professional sophistication, and its ambitious selection of targets.

Events such as the Stuxnet attack, severely damaging Iran's centrifuges, and the widespread protest that accompanied the 2009 elections in Iran – in which social networks and the internet played a major role in organizing protests and escalating events – have turned cyberspace into an important theater for the Iranian regime. These events and other cyber-attacks against Iran have led the regime to establish a ramified cyber apparatus, including operational frameworks with a command structure and professional echelon specializing in a variety of areas. Iran has invested over $1 billion in developing technologies, setting up infrastructure, and training defensive and offensive personnel.[2] Iranian cyber strategy is devised and overseen at the highest levels, among them the President, commander of the Revolutionary Guards, and senior ministers serving on the Iranian Supreme Cyberspace Council – the senior agency coordinating the country's cyber activity.[3]

This article seeks to present an up-to-date analysis of Iranian activity in cyberspace. The article is divided into two parts; the first examines Iran's cyber defense system's progress and activity, and the use of these capabilities to restrain its internal opposition. The second examines the offensive dimension, mainly through cyber-attacks traced to Iranian agencies, agents, and allies. Concluding insights are provided at the end of the article.

The Defensive Concept

Iran is aiming to create a multi-level defense system combining security, monitoring, and supervising technologies with physical enforcement mechanisms for the aggressive pursuit of operatives operating against the regime in cyberspace. To this extent, Iran is taking action through three main channels: first, it is creating a protective envelope against attacks on its essential infrastructure and sensitive information, such as the Stuxnet attack that damaged its uranium enrichment program. Second, it is striving to neutralize cyber activity executed by opposition groups and opponents of the regime, for whom cyberspace constitutes a key platform for communications, information distribution, and organized actions against the regime. Third, it aims to prevent harmful Western content and ideas from infiltrating Iran's internal cyberspace – ideas that could contribute to the development of a "soft revolution," undermining the regime's stability.

The targets and operational principles of the Iranian cyber defense apparatus, dictated by Iran's Supreme Council of Cyberspace, are implemented by central government agencies, such as the Passive Defensive Organization (belonging to the army), the Supreme Council of the Cultural Revolution (subject to the Supreme Leader), the Iranian Police, and Ministry of Communications.[4] Some of the technological and organizational infrastructure established by Iran has matured during the past year into operational agencies significantly contributing to strengthening Iranian defensive operations in cyberspace.

The Networks Isolation Project – Disengagement from the World

The Networks Isolation Program is one of the Iranian regime's main strategies in cyberspace. The project began materializing as early as 2009, when Iran's objective was to transfer the cyber activity in the country to an internal communications network, dubbed Halal Internet, isolated from the World Wide Web. The Iranian network was designed to operate in the spirit of the Shiite Muslim norms encouraged by the regime, and to enable the government to completely control and supervise the network's content, information, and users. From the regime's perspective, the establishment of an intranet network and the separation of Iranian cyberspace from global cyberspace is a key measure in strengthening its defense against cyber-attacks and espionage, preventing penetration by Western elements that do not coincide with those of the regime, and neutralizing its internal opposition.[5]

The first evidence of the Iranian network's operation was discovered in October 2012, when American cyber researchers, in cooperation with Iranian sources, noticed that Iranian Internet providers have begun allocating two IP addresses to every computer connected to the Internet – an ordinary internet address and an internal Iranian address, which could be accessed only from inside the country. The researchers estimated that the internal Iranian network was capable of managing 17 million IP addresses and that more than 10,000 home, commercial, and government computers were connected to it during 2012. In 2013, Halal Internet began to accumulate content (censored and supervised, of course), with a strong emphasis on development of local versions of popular internet services, such as e-mail, social networks, video and audio communications, map websites, and video websites.[6]

In July 2013, the Iranian regime inaugurated an e-mail service, @post.ir, requiring civilians to register and designed to constitute the main channel of communication between private citizens and the various governmental agencies. This service, which supports Farsi, English, French, and Arabic, is capable of providing e-mail addresses to about 100 million users. Each user is allocated a 50-megabyte mailbox, which can be expanded to up to two gigabytes. Opening the mailbox requires a person to give his name and address, and it appears that the email addresses provided are not encrypted – therefore enabling the regime to closely supervise the users and traffic in these addresses.[7] In December 2012, the Iranian State Broadcasting Authority launched a YouTube-like website under the name of "Mehr," displaying supervised content and enabling surfers to upload their own content under strict censorship rules.[8] The Iranian authorities also banned the use of foreign Information Security software, as they developed a local anti-virus system called "Padvish." According to Iranian sources, this system can protect networks and prevent malware penetration.[9]

In order to increase the number of Halal Internet and Iranian Internet services' users, the regime expanded its use of technological and legislative measures restricting Iranian citizens' possibilities for accessing the World Wide Web. The Iranian authorities blocked the use of Voice-over-IP software, such as Skype and Google Talk. Use of many VPN and TOR networks as well as filtering evasion software, important tools in bypassing government supervision and censorship of cyberspace, was also banned.[10] In addition, the Iranian cyber authorities began to deliberately slow external websites and Internet services (mainly services by Google, which are very popular in Iran), at times reaching 6 percent of the ordinary speed. The authorities are also carrying out websites and services migrating blocks, and are greatly restricting traffic on the encrypted Internet. These actions pose technical, legal, and psychological difficulties for Iranian citizens seeking to surf the World Wide Web, and are, in effect, forcing them to use the supervised and censored Halal Internet.[11]

Development of Defense and Supervision Technologies

As a supplementary measure to isolating the networks, Iran is investing in the development of its own cyber technologies and defense tools in order to reduce its dependence on foreign products that may prove to be Trojan Horses. A well-publicized ceremony attended by senior Iranian defense officials, including Minister of Defense General Hossein Dehqan and Civil Defense Unit Commander Gholam Reza Jalali in December 2013 unveiled 12 technological developments by Iranian industry, including a secure cellular telephone designed to provide users with a communication line impenetrable by electronic surveillance, a secure operating system designed to eliminate Iranian dependence on American operating systems, a GPS device, an optical communications system, software and systems against malware and a firewall. A system for identifying a cyber-attack, and equipment for information security centers were also unveiled at the conference.[12] Furthermore, the Iranian news agency ISNA reported that Iran had begun using a national cyber protection system called "Shahpad." According to Mohammed Naderi, head of the project, the system facilitates fusing information from a variety of user stations and sensors, and generates an overall nationwide cybernetic picture. In case of an attack, Shahpad immediately informs the data security centers in the country, enabling them to respond quickly, and to take action to block the attack.[13]

Iran is not relying solely on local development in order to reinforce its cyber security capability. In September 2012, it signed an extensive technology cooperation agreement with North Korea including information technology. According to experts, it is very likely that the two countries that have both been targets of cyber-attacks, and both regard this field as strategically important, will combine forces under this agreement to develop information security, monitoring, and even offensive technologies.[14]

Iran is also cooperating with China in the cyber field, and previously purchased a surveillance system from a Chinese company named ZTE Corp., making it possible to monitor voice communications, text messages, and Internet browsing.[15] Cooperation with these and other countries, such as Russia, is of great assistance in strengthening Iran's cyber defense and ability to conduct surveillance of the Internet and its own citizens' usage.

Strengthening Defensive Deployments

Beyond the technological aspects, Iran is placing special emphasis on reinforcing various state agencies' ability to face and thwart cyber-attacks. The Iranian cyber apparatus had conducted a number of comprehensive cyber defense drills training civilian and military units. In addition, a cyber-war exercise was conducted as part of naval maneuvers by the Revolutionary Guards in the Strait of Hormuz in December 2012. As part of this exercise, a cyber-attack was launched against the fleet's computer network in order to retrieve information and insert malware. The commanders of the exercise declared that the attack had been detected and foiled by the fleet's cyber defense system.[16]

In February 2013, the Iranian Fars News Agency, which is close to the regime, reported a comprehensive drill by the Revolutionary Guards' ground forces, examining and assessing the organization's cyber defense systems.[17] Another drill took place in October 2013 as part of the Passive Defense Organization's general defense maneuvers. As part of this drill, key government agencies' cyber defense apparatuses were examined, including nuclear installations, the Tehran metro subway network, the Iranian Broadcasting Authority, ports, the Iranian Central Bank, and the cellular communications' providers. According to the Passive Defense Organization commander, many security breaches in these organizations' cyber defense systems were found and managed. Following the drill, it was decided to establish a cyber-defense center at the Natanz nuclear facility.[18]

Restraining Regime Opponents

Iran is supplementing the technological measures it is taking in order to protect its cyberspace with aggressive physical enforcement action against its opponents at home, who use cyberspace extensively for subversive purposes. A key player in the Iranian regime's efforts to control its cyberspace is FATA, the Cyber Police, founded in 2011 under the command of the Iranian Police. Over the past year, FATA has become more aggressive in its efforts to enforce censorship restrictions and prevent subversive activity in cyberspace. The agency is engaged in locating and apprehending bloggers, online journalists, and opposition members supporting and voicing ideas and views that run contrary to the regime's positions.

The intense aggression against the regime's opponents exhibited by the Iranian Cyber Police gained global attention in November 2012, following reports of the death of Iranian blogger Sattar Beheshti in a prison near Tehran. Beheshti, who was arrested by FATA after he published a blog voicing criticism of the Iranian legal system (which he called "Khamenei's Slaughterhouse"), died as a result of torture and severe beating by the Cyber Police.[19] Reports of his death aroused a wave of criticism both within and outside Iran. As a result, the European Union imposed sanctions on FATA and other parties involved in his death, including judges and officials responsible for censorship in Iran.[20] International pressure led to the dismissal of the Cyber Police commander in Tehran,[21] but according to international human rights organizations, FATA is persisting in its strategy of widespread arrests and aggressive action to locate and punish Iranians expressing opposition to the regime on social networks and in blogs.[22] In recent months, the Iranian Cyber Police tightened its supervision of the popular Internet Cafes, closing dozens for violating the state's stringent registration laws and restrictions.[23]

The regime's supervision and enforcement became particularly intensive and thorough in the months leading up to the presidential elections on June 14, 2013. Two days prior to the elections, Google reported that it had detected and thwarted a phishing attack launched by parties inside Iran aimed at tens of thousands of e-mail accounts belonging to Iranian citizens. The attack included sending an e-mail disguised as a maintenance message from the Gmail system asking the user to type in his e-mail user name and password. The information typed was then transferred directly to the attackers, providing them with untrammeled access to the user's e-mailboxes.[24] An analysis of the attack raised the suspicion that the attackers were the same Iranians who attacked the Dutch DigiNotar company's servers in 2011.[25] The attackers' targets were unclear, though it appears there is a close connection between the attack and the election campaign, and that the attackers wanted to enable the Iranian authorities to collect information about the actions and opinions of Iranian citizens, and to take action against "problematic" elements.[26] In addition, in the weeks leading up to the elections, a broad cyber-attack took place against Iranian opposition and communications websites. A group of hackers calling itself "The Unknown Cyber Jihad," and, claiming affiliation to Hizbollah, broke into a number of Iranian opposition websites and replaced their content with a message aimed against the regime's opponents. Key opposition websites, such as the Communist Movement in Iran, the Green Movement, and human rights websites, were blocked by the regime for many hours, and dozens of online activists and journalists were arrested and imprisoned by the Iranian security forces.[27]

Following the events that accompanied Ahmadinejad's re-election in 2009, Iranian activity against the opposition and opponents of the regime has developed and become more advanced. At the time, the opposition used cyberspace with relative ease to organize demonstrations, distribute ideas, and transmit information about events in Iran to a target audience outside of the country (mainly through the use of VPN networks). In the

2013 elections, however, the Iranian cyber apparatus was technologically and operationally prepared and ready to control the dialogue that took place on the internet, and monitor subversive activity and the outwards flow of information from within Iran.

It appears that to date, the Iranian cyber defense system still has a long way to go before it is able to deal effectively and consistently with highly sophisticated cyber-attacks, such as Stuxnet and Flame, and to prevent any penetration by external content or ideas. Some describe this apparatus as no more than an improvised and less organized version of the Chinese "Cyber Wall."[28] Nevertheless, the great technological and organizational strides that Iran has made over the past year indicate a steep learning curve, and that it is likely to devise an effective and comprehensive defense system earlier than expected.

The Offensive Aspect – The Search for "High-Quality" Attacks

The Islamic Republic of Iran regards cyber warfare as an effective platform enabling it to inflict damage on enemies in possession of clear military superiority, while at the same time maintaining room for denial in order to avoid international condemnation, or even sanctions and counterattacks. This conception had led Iran to use cyber warfare as an important tool for attacking Western targets in response to sanctions, and as a means of deterrence against escalating sanctions actions against Iran by Western countries. The scope, targets, and relative success of cyber-attacks conducted over the past year and their attribution to Iranian groups indicate increased Iranian capabilities. Intelligence and administration officials in Israel and the US have also expressed concern regarding the speed of Iranian cyber warfare capabilities' development.[29]

Western sources attribute the progress in Iran's cyber warfare program to its success in integrating its capabilities, know-how, and trained personnel from Iranian computer science faculties[30] with the Iranian hacker community's extensive experience and highly developed abilities, many of whose members identify with the regime and its goals. The Iranian hacker community is one of the most dominant and active communities worldwide, and evidence suggests connections between its various groups and the Revolutionary Guards. The use of hackers, whose connections to the Iranian regime are vague, provides room for ambiguity and deniability when facing accusations of involvement in malicious and illegal cyber activity.

One of the leading Iranian hacker groups is the Ashiyane Digital Security Team, which is believed to have connections with the Revolutionary Guards, and whose members are ideologically motivated to support the Iranian regime and the revolution.[31] The Zone-H website, specializing in analyzing hacker activity in cyberspace, rates Ashiyane as second in the world in the number of websites into which its members have succeeded in breaking and corrupting, usually by replacing the content with the group's icon, or with pro-Iranian propaganda. The websites broken into by Ashiyane members include 26 Brazilian government websites, among them the Military Police website, and government websites in the UK and Pakistan.[32] According to Zone-H, besides Ashiyane, there are seven other Iranian hacker groups among the world's 40 most active hacker groups involved in corrupting websites. Such attacks are considered relatively minor, but they indicate a high level of technological capabilities, and in many cases serve as cover for information theft or introduction of malware and Trojan Horses.

Another factor contributing to the Iranian cyber warfare program's rapid progress is the Iranian cyber system's close relations with cyber criminals, hackers, and information security experts, primarily Russian, who are willing to hire out their capabilities for money. American sources regard these connections as a key element in Iran's rapid progress, and Congressman Michael Rogers, Chairman of the House of Representatives Select Committee on Intelligence, also stated that the wave of cyber-attacks against American banks' websites, which was attributed to Iranian groups, showed signs of involvement by Russian groups.[33] In addition to "importing" personnel, Iran can also purchase a powerful and technologically sophisticated cyber weapon which is available on the black market to the highest bidder. This Cyber Weapon enables the Iranians to rapidly enhance their capabilities and the threat posed by them.[34]

The Iranian cyber warfare capabilities' progress is reflected in a series of attacks that occurred in the second half of 2012 and in 2013, utilizing more sophisticated techniques, attacking high quality targets, and on a larger scale than earlier attacks attributed to Iran. One attack attributed to Iranian groups began in September 2012 and continued into 2013, including a large-scale attack on the websites of key banks and financial institutions in the US. Information security experts described this attack as "unprecedented in scope and effectiveness." Its uniqueness and quality lay in the method employed by the attackers: instead of attacking through breaches in individual computers, they routed their attacks through data centers' computer networks. These data centers, operated by companies like Google and Amazon.com, are composed of giant computer networks connecting hundreds, sometimes thousands, of servers and computers, providing cloud computing services to a large number of companies and businesses throughout the world. The attackers succeeded in taking over part of these computing "clouds," utilizing their enormous computer power as a platform for attacks on the websites of US-based banks and financial companies. Security specialists described this maneuver as the "cybernetic equivalent of turning a Chihuahua into a fire-spitting Godzilla."[35]

A group of hackers calling itself Izz a-Din al-Qassam Cyber Fighters assumed responsibility for the service-denying attack against the websites of important banks in the US, which included Bank of America, Citigroup, and HSBC. Members of the group exploited the data centers' computer platform to channel enormous volumes of traffic to the banks' websites, causing them to crash and denying their customers access to their accounts. In addition to using traffic, the attackers employed a technique called Encrypted DDos (distributed denial of service). This method exploits the banks' own information encryption mechanisms, whose operation requires major system resources. The attackers flooded the banks' websites with transactions requiring encryption, thereby substantially slowing and hindering their activity. Nevertheless, the bank accounts were not broken into during the attacks, and customers' money was not stolen.[36]

Information security experts state that the high level of capabilities required to carry out an attack on such a large scale and with such great technological sophistication indicates that a country must be involved. An attack against a country's financial infrastructure, especially an economic power like the US, has serious consequences, and is liable to cause severe economic damage as it disrupts many commercial companies and households' regular financial activity.

Despite Iranian denials and the absence of physical proof, senior US administration and intelligence officials are convinced that Iran is behind the attacks as a response to the international sanctions against it and the cyber-attacks that damaged its infrastructure, for which it holds the US and Israel responsible. The US Secretary of Defense at the time, Leon Panetta, commented on the attacks against the banks, saying that they constituted a "significant escalation," without mentioning Iran by name.[37]

Another wave of attacks attributed to Iranian groups focused on American infrastructure and energy companies. It began to gather steam in early 2013, until the US Department of Homeland Security decided in May 2013 to issue an exceptional warning to energy and infrastructure companies regarding the escalating cyber threat to their computer networks. This warning stated that these were not routine attacks for the purpose of stealing information, industrial espionage, or inflicting damage on administrative systems; they were attacks seeking to gain control of their systems and damage their physical operations or the safety equipment of critical infrastructure, such as oil and gas pipelines and electrical systems. The American administration did not officially declare Iranian involvement, but experts and administration officials said that there was operational evidence indicating that the attacks had originated on Iranian soil, and that carrying them out required at least some support from the agencies in charge of Iranian cyberspace.[38] Any future sanctions escalation against the Iranian energy market is likely to cause Iran to take strategic measures against the international energy market, both as a deterrent measure and in order to increase the demand for its oil. [39]

Experts describe the attacks on the American energy companies' computer networks as a large-scale information collection operation, learning and assessing the systems in order to create knowledge infrastructure and gain experience in preparation for a future attack on the control systems that operate and regulate critical infrastructures' activity. Harming these systems is liable to cause significant damage and even loss of life on a large scale. Indeed, in the course of the attack, the attackers succeeded in bypassing some of the security systems and collecting information about their structure, capabilities, and their security breaches.[40] A senior source in Mandiant, an Information Security company, said that in at least one case, its investigators had succeeded in tracing the attack to a group of Iranian hackers whose connections with the regime were unclear. He added that the attackers' goal, moving within the American computer systems and studying their detection and security array, was to accumulate experience with "live" networks, and to explore their weak points.[41] Senior American officials stated that the attacks against the energy companies and the hackers' relative success indicated that the cyber offensive capabilities at the Iranians' disposal were improving and developing rapidly.[42] If Iran obtains effective offensive capabilities against essential infrastructure systems' control, this is likely to constitute a strategic threat to its enemies.

Another significant attack attributed to Iran occurred in September 2013, when official US sources reported that an unclassified US Naval computer network had been compromised. The sources said that the attack had been committed by a group of hackers operating in the service of the Iranian regime, or at least with its consent and support. The network affected was the fleet's internal network, which, while unclassified, is used for correspondence and communications, among other things, and contains sensitive information, such as e-mail addresses of the fleet commanders and of senior officials. Administration sources reported that the attackers had succeeded in penetrating the network management systems, but claimed that no significantly valuable information had been stolen, and that e-mailboxes had not been broken into. Particularly alarming was the fact that the hackers continued operating in the fleet's computer network even after American security agencies had reported their successful removal from the network. The Iranian sophistication revealed in this attack is another sign of the development and progress in Iran's infiltration capabilities, and of Iran's readiness to target military cyber systems.[43]

In addition to the series of attacks against American institutions, groups affiliated with Iran assumed responsibility during the past year for cyber-attacks against Israeli institutions. In June 2013, Prime Minister Benjamin Netanyahu announced that there has been a steep rise in the Iranian cyber-attacks against important computer infrastructure in Israel.[44] In December 2013 and January 2014, a group of Islamic hackers calling itself The Islamic Cyber Resistance Group (ICRG) claimed that it had conducted a number of high-quality attacks against targets in Israel and the Middle East in revenge for the killing of senior Hezbollah leader Hassan al-Laqqis. The group, extensively publicized by the Iranian Fars News Agency, claims that it managed to penetrate the Israeli Civil Aviation Authority control systems, and was able to remain undetected within the system for months. In addition, the group claimed that it had succeeded in stealing sensitive information, and could, had it chosen to do so, take over the Authority's navigation and communications systems causing an air disaster.[45] ICRG also proclaimed that it had succeeded in penetrating the IDF computer servers, stealing secret information, such as the personal files of IDF soldiers, lists of officers, passwords, residential addresses and e-mail addresses, and military codes. Aside from the attacks against Israel, ICRG announced that it had managed to break into the Saudi Arabian army database and the computers of companies owned by the Bin Laden family.[46] At the same time, sources in Israel stated that the rumored attacks boasted by the group were false, and were no more than propaganda and psychological warfare on the part of Iran.

In the midst of these events is the mysterious death of Revolutionary Guardsman Mojtaba Ahmadi, found dead in early October 2013. Reports in the West indicated that he had served as commander of the Revolutionary Guards' Cyber War Headquarters. His death was attributed to Israel at first, but the Revolutionary Guards strongly denied this allegation, stating that his death had resulted from a "strange accident."[47] Despite the great obfuscation surrounding this event, the possibility that Ahmadi's death had consequences for the organization's activity in the cyber sphere cannot be ruled out.

The Cyber Warfare Agents

Along with Iran's government cyber apparatus and its cooperation with the hacker community, Iran is redoubling its attempts to expand and strengthen its allies' cyber capabilities. It appears that Iran is seeking to create an effective system of agents acting in cyberspace on its behalf. One of its main foci in this area is Syria, which has strategic importance for Iran. At the beginning of the conflict between the Assad regime and the rebel forces, the Iranians began to finance, equip, and train the Syrian security forces in methods of monitoring and controlling cyberspace, used by the rebels as a an important platform for organizing activity against the regime. Iranian advisers and specialists trained and reinforced the Syrian cyber police, and helped conduct surveillance of the computer and cellular networks in the country, thereby damaging the rebel's ability to transmit messages and information, both within and outside the country.[48]

A key player in this context is the Syrian Electronic Army (SEA). This group of Assad-supporting hackers began operating in 2011. During its first year of activity, it conducted mainly relatively amateurish vandalizing attacks against low-security websites that did not require significant technical ability: spam attacks, flooding talkback systems of various forums and news websites, etc.[49] In 2012, SEA began executing more complex operations against websites with a higher level of security, requiring greater technical knowledge and capabilities. Western cyber experts and administration officials attribute this major improvement to the involvement and instruction of Iranian cyber warfare experts, training and equipping SEA's operatives. Former CIA Director and NSA Director Michael Hayden also stated that the Syrian group of hackers was for all intents and purposes, an agent of Iran.[50]

The development of SEA was reflected over the past year in a wave of attacks against communications agencies and human rights organizations' websites, perceived as hostile to the Assad regime. Among other things, SEA members attacked leading news websites, including the *New York Times*, BBC, al-Jazeera, the *Washington Post*, and the *Huffington Post*. The organization also attacked the Human Rights Watch website, which provides information about the number of civilians killed in battles in Syria. In addition, members of the organization succeeded in causing substantial damage when they took over the AP news agency's Twitter account, and published a false report about a supposed attack on the White House that injured President Obama. The report generated immediate panic on Wall Street, causing a nosedive in share prices and damage estimated at $136 billion. In April 2013, SEA assumed responsibility for crashing the Twitter Social Network, and for channeling surfers from the US Marines' recruitment website to a propaganda website against the rebels.[51]

Recently, it appeared that SEA had exhibited another major advance in its capabilities, and was beginning to use more sophisticated techniques and tools, such as phishing, malware, and Trojan Horses. Such tools have enabled the organization to carry out high-quality attacks against Internet communications companies' servers, such as TrueCaller which is the world's largest telephone index; the messaging and video service company Tango, and the communications applications company Viber. In the course of these attacks, the attackers succeeded in stealing huge quantities of information, such as personal information and e-mail addresses, which may very well have been handed over to Syrian intelligence and used to target the regime's opponents as well as for espionage.[52] The Iranian Fars News Agency also reported that the organization had attacked the water system of the city of Haifa,[53] but pictures attached to the report showed that SEA had merely penetrated the irrigation control system of a community in northern Israel.[54] Nevertheless, the attack on and penetration of the control system of Israeli infrastructure indicates an attempt by SEA to utilize and target more advanced cyber warfare methods.

These advanced capabilities, which many experts regard as the result of Iranian training, guidance, and assistance, have turned SEA into significant actor in the cyberspace arena, and have made cyber warfare in general a crucial element in Syria's deterrence strategy. When Syria sought to deter an American attack in response to the use of chemical weapons by Assad's forces, SEA operatives sent a message to the Reuters news agency saying that in the event of an American attack in Syria, the organization would escalate its attacks, and take action against more significant targets. Richard Clarke, Former US National Coordinator for Security, Infrastructure Protection, and Counter-terrorism and Special Advisor to the President on Cyber Security said that if the US attacks Syria, every response by Syrian agencies in cyberspace would be facilitated by Iranian groups.[55]

In addition to its support of the Assad regime's cyber capabilities, Iran continues its traditional support for its satellite and closest ally, Hizbollah's cyber deployment, which has become an active player in attacking Israel.[56] A report by the Meir Amit Center indicates intensive involvement and support by Iran for the Hizbollah's array of websites. These sites constitute a platform for propaganda and indoctrination in the ideas of the Islamic Revolution, including pro-Iranian propaganda, the glorification of Supreme Leader Khamenei and Hizbollah leader Hassan Nasrallah, and anti-Israel and anti-Semitic propaganda. The content of these websites was determined in cooperation with Iran, subject to the Iranian propaganda strategy. Part of the content is even operated from Iranian territory by parties close to the regime.[57]

Concluding Insights

Iran's cyber warfare capabilities are continuously progressing. Iran already constitutes a significant factor whose intentions should not be held lightly. It can be stated that the Iranian decision to operate in cyberspace on a large scale is due to two main considerations; the first is its experience as the target of serious cyber-attacks. As a country that had experienced the power and capabilities of a cybernetic attack, Iran recognizes the importance of establishing defensive capabilities and building and using attack capabilities. Iran's other motive concerns global technological development, allowing the expansion of its range of actions into cyberspace, in addition to the physical world. This development optimally fits in with Iran's asymmetric strategy concept.

An analysis of the cyber-attacks attributed to Iran and its satellites shows a broad range of targets, goals, and methods. One of the conclusions arising from this article is that Iran's cyber capabilities have recently matured on both offensive and defensive levels. Although it is likely that these capabilities are still inferior to those of the leading technological powers, it appears that the Iranians are bridging the gaps quickly and effectively.

One of the most dangerous trends in Iran's offensive cyber activity is its ability to target organizations and countries' core operational systems. These systems, controlling and overseeing manufacturing processes, supplies and essential services, are liable to be targets of Iranian attacks. Exploratory, scanning and learning actions discovered in the American energy companies' computer systems and traced to Iranian groups can be interpreted in only one way: Iran is trying to attain the capability and accessibility needed for an attack on critical infrastructure. This accessibility may avoid detection altogether, and can be utilized in the future for offensive purposes if Iran so decides. A successful attack on the energy, gas, and water facilities' control systems is liable to cause substantial damage. In the framework of the rules of the game, espionage and information theft in cyberspace is seemingly tolerable, but attempts to penetrate civilian infrastructure control systems cannot and should not be accepted. These attempts require a decisive response.

It appears that the realization that Iran poses a significant threat to its enemies in cyberspace is already inspiring close cooperation between the countries threatened by these capabilities. Upgrading intelligence and producing better defensive capabilities are not enough, however; they will never suffice against a determined enemy with operational, intelligence, and technological capabilities. Cyberspace makes possible a range of channels through which one can transmit messages below the threshold of physical warfare. These actions will require demonstration of the damage that Iran may suffer should it continue to act without restraint against sensitive targets. Particular information was recently published regarding a large-scale cyber offensive operation in Syria prepared by NSA in the spring of 2011, immediately following the outbreak of the Syrian civil war.[58] If this report is correct, the preparation of a cybernetic strike against Iran, combined with the occasional demonstration of qualitative capabilities, can help restrain its actions in the area of critical infrastructure.

Until a magic technological formula is found for identifying the source of cyberspace attacks at a level of certainty that can be legally proven, circumstantial evidence of the source of the attack can suffice in quite a few cases, and strong action in cyberspace below the physical warfare threshold can be taken against this source.

Above all, closer cooperation between the democratic countries is a cornerstone in facing Iran and its satellites. Better operational, intelligence, and technological connections are essential, as well as improvement in information sharing regarding the methods and tools used by Iran and its satellites. In addition, Israel is also likely to find allies against Iranian cyber warfare among the Sunni regimes in the Persian Gulf, headed by Saudi Arabia, which is under continual threat, and which has been damaged in the past by Iranian agencies. The cyber defense realm, in which Israel is a leader, is likely to serve as a basis for a fruitful strategic dialogue on broader regional issues, such as the Iranian threat in its general sense, the crisis in Syria, and the Palestinian issue.

The Iranian cyber deployment's aggressive behavior highlights the totalitarian character of the Iranian regime. Tight and intrusive supervision that violates the freedom of speech and expression of Iranian citizens, combined with the violence and aggression typical of agencies such as the Cyber Police, refute the image that the Rouhani regime is seeking to promote in order to break the international sanctions regime against Iran. Israel and other countries can use Iran's activities in cyberspace as an explanatory platform for highlighting the totalitarian and aggressive nature of the Islamic Republic.

This reality of Iran's rapid cyber warfare capabilities' development, its satellites, and its allies require Israel and other Western countries to act methodically and with determination to maintain their qualitative and operational edge in cyberspace. The importance of this space for Israel's security concept and the urgency of creating a "digital Iron Dome" were strongly emphasized by IDF Chief of Staff Lt. General Benny Gantz, who said he believed that Israel needed to do a lot more in the cyber realm: "We must not wait with this story."[59]

Notes

1 Barbara Slavin and Jason Healey, "Iran: How a Third Tier Cyber Power Can Still Threaten the United States," The Atlantic Council, 2013, http://www.atlanticcouncil.org/images/publications/iran_third_tier_cyber_power.pdf.

2 Yaakov Katz, "Iran Embarks on $1b. Cyber-Warfare Program," *The Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864.

3 Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare," *Military and Strategic Affairs* 4, no. 3 (2012): 77-99.

4 Ibid.

5 Majid Rafizadeh, "Iran's 'Halal' Version of the Internet," *al-Arabiya News*, July 12, 2013, http://english.alarabiya.net/view-renderer?mgnlUuid=cb92c5e3-f973-45ce-8d46-12b8fb4dfe17.

6 Sara Reardon, "First Evidence for Iran's Parallel Halal Internet," *New Scientist*, October 10, 2012, http://www.newscientist.com/article/mg21628865.700-first-evidence-for-irans-parallel-halal-internet.html#.UnZubT4UHVI.

7 Saeed Kamali Dehghan, "Iran Launches 'National Email Service,'" *The Guardian*, July 9, 2013, http://www.theguardian.com/world/2013/jul/09/iran-launches-national-email-service.

8 "Iran launches Own 'YouTube' Website," *AFP*, December 9, 2012, http://en-maktoob.news.yahoo.com/iran-launches-own-youtube-website-121634740.html.

9 F. Karimov, "Iran Introduces Domestically-Made Antivirus Padvish," *Trend News Agency*, June 30, 2013, http://en.trend.az/capital/it/2166121.html.

10 This blocking was accomplished, among other ways, by deliberately distributing malware disguised as filtering evasion software, which enabled the regime to trace illegal networks.

11 Urt Hopkins, "Why Iranians might Actually Use the Censored Halal Internet, " *The Daily Dot*, April 25, 2013, http://www.dailydot.com/society/iran-halal-private-internet-blocked-censorship; "Iranian Internet Infrastructure and Policy Report," *Small Media*, February-March 2013, http://smallmedia.org.uk/InfoFlowReportMARCH.pdf.

12 "Iran Unveils 12 Cyber Products," *Fars News*, December 14, 2013, http://english.farsnews.com/newstext.aspx?nn=13920923001322.

13 "Iran Launches Home-Made Defence Shield," *ISNA*, December 9, 2013, http://isna.ir/en/news/92091812343/Iran-launches-home-made-defense-shield.

14 Alastair Stevenson, "Iran and North Korea Sign Technology Treaty to Combat Hostile Malware," V3, September 3, 2012, http://www.v3.co.uk/v3-uk/news/2202493/iran-and-north-korea-sign-technology-treaty-to-combat-hostile-malware#.

15 Steve Stecklow, "Chinese Firm Helps Iran Spy on Citizens," *Reuters*, March 22, 2012, http://graphics.thomsonreuters.com/12/03/IranChina.pdf.

16 "Iran for the First Time Stages Cyber Warfare Drill," *al-Arabiya*, December 31, 2012, http://www.alarabiya.net/articles/2012/12/31/257960.html.

17 "Drones, Cyber-Defence Feature in Iran Guards Drill," *Jerusalem Post*, February 23, 2013, http://www.jpost.com/Iranian-Threat/News/Drones-cyber-defense-feature-in-Iran-Guards-drill.

18 N. Umid, "Iran Holds Defence Exercises," *Trend News Agency*, October 22, 2013, http://en.trend.az/news/politics/2203465.html; "Iran Carries out Drills to Detect Cyber Vulnerabilities," *Tasnim News Agency*, October 22, 2013, http://www.tasnimnews.com/english/Home/Single/172473.

19 "Iranian Blogger who Told Supreme Leader Khamenei 'Your Judicial System... is nothing but a Slaughterhouse' Tortured to Death in Prison," *MEMRI*, November 19, 2012, http://www.memri.org/report/en/0/0/0/0/0/0/6819.htm.

20 European Parliament, *Resolution of November 22, 2012 on the Human Rights Situation in Iran, Particularly Mass Executions and the Recent Death of the Blogger Sattar Beheshti*, November 22, 2012, http://www.europarl.europa.eu/document/activities/cont/201301/20130109ATT58696/20130109ATT58696EN.pdf.

21 Thomas Erdbrink, "Head of Tehran's Cybercrimes Unit is Fired over Death of Blogger," *The New York Times*, December 1, 2012, http://www.nytimes.com/2012/12/02/world/middleeast/after-death-of-sattar-beheshti-iranian-blogger-head-of-tehrans-cybercrimes-unit-is-fired.html.

22 "Intelligence Ministry Admits Arresting News Providers, Blames Foreign Media," *Reporters Without Borders*, February 20, 2013, http://en.rsf.org/iran-intelligence-ministry-admits-20-02-2013,44099.html ; "Iran: Two Arrested for 'Insulting Regime Officials' on their Facebook Page, "*National Council of Resistance of Iran*, July 10, 2013, http://www.ncr-iran.org/en/news/human-rights/14138-iran-two-arrested-for-insulting-regime-officials-on-their-facebook-pa.

23 "Tehran Closes Dozens of Internet Cafes," *Mohabat News*, July 27, 2013, http://www.mohabatnews.com/index.php?option=com_content&view=article&id=7222:tehran-closes-dozens-of-internet-cafes&catid=35:inside-iran&Itemid=278.

24 Eric Grosse, "Iranian Phishing on the Rise as Elections Approach," *Google Blog*, June 12, 2013, http://googleonlinesecurity.blogspot.co.il/2013/06/iranian-phishing-on-rise-as-elections.html.

25 Siboni and Kronenfeld, "Iran and Cyberspace Warfare."

26 Betsy Isaacson, "Iran's Pre-Election Phishing Scheme Detected, Disrupted by Google," *Huffington Post*, June 13, 2013, http://www.huffingtonpost.com/2013/06/13/iran-phishing-google_n_3435811.html.

27 "Iranian Authorities Target Internet, Media before Elections," *CPJ*, June 13, 2013, http://www.cpj.org/2013/06/iranian-authorities-target-internet-media-

before-e.php; Helle Dale, “Iran Clamps down on Dissidents before Election,” *The Foundry*, June 12, 2013, http://blog.heritage.org/2013/06/12/iran-clamps-down-on-dissidents-before-election.

28 Neal Ungerleider, “Iran’s ‘Halal Internet’ is really a ‘Filternet,’” *Fast Company*, 2013, http://www.fastcompany.com/3009714/irans-halal-internet-is-really-a-filternet.

29 Thom Shanker & David E. Sanger, “U.S. Helps Allies Trying to Battle Iranian Hackers,” *New York Times*, June 8, 2013, http://www.nytimes.com/2013/06/09/world/middleeast/us-helps-allies-trying-to-battle-iranian-hackers.html?nl=todaysheadlines&emc=edit_th_20130609&_r=4&pagewanted=all&.

30 Siboni and Kronenfeld, “Iran and Cyberspace Warfare.”

31 Frank J. Cilluffo, “The Iranian Cyber Threat to the United States,” *A Statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cybersecurity, Infrastructure, Protection and Security Technologies*, April 26, 2012, p. 5.

32 “Brazilian Military Police & 26 Govt Websites Hacked by Ashiyane Digital Security Team,” *Hackread*, January 28, 2013, http://hackread.com/brazilian-military-police-26-govt-websites-hacked-by-ashiyane-digital-security-team.

33 Julian E. Barnes and Siobhan Gorman, “U.S. Says Iran Hacked Navy Computers ,” *The Wall Street Journal*, September 27, 2013, http://online.wsj.com/news/articles/SB1000142405270230452620457910160235675172; Adam Kredo, Mike Rogers, “China, Iran and Russia Launching Cyber Attacks Against U.S. ,” *The Washington Free Beacon*, July 22, 2013, http://freebeacon.com/mike-rogers-china-iran-and-russia-launching-cyber-attacks-against-u-s.

34 Shanker and Sanger, “U.S. Helps Allies Trying to Battle Iranian Hackers.”

35 Nicole Perlroth and Quentin Hardy, “Bank Hacking Was the Work of Iranians, Officials Say,” *The New York Times*, January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?pagewanted=1&_r=1&ref=iran&&version=meter+at+6&region=FixedCenter&pgtype=Article&priority=true&module=RegiWall-Regi&action=click.

36 Ibid.

37 Julian E. Barnes and Siobhan Gorman, “Iran Blamed for Cyberattacks,” *The Wall Street Journal*, September 27, 2013, http://news.walla.co.il/?w=/15/2569449, “Iran Launches Powerful Cyber Attack against Banks in US,” Walla!, January 9, 2013, http://news.walla.co.il/?w=//2605254.

38 Ellen Nakashima, “U.S. Warns Industry of Heightened Risk of Cyber Attack,” *The Washington Post*, May 10, 2013, http://www.washingtonpost.com/world/national-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html; see also an analysis of the capabilities required to carry out a high level

cyber-attack: Gabi Siboni, Daniel Cohen, and Aviv Rotbart, "The Threat of Terrorist Organizations in Cyberspace," *Military and Strategic Affairs*, Volume 5, No. 3, Institute for National Security Studies, December 2013, http://d26e8pvoto2x3r.cloudfront.net/uploadImages/systemFiles/The%20Threat%20of%20Terrorist%20Organizations%20in%20Cyberspace.pdf; Nicole Perlroth and David E. Sanger, "New Computer Attacks Traced to Iran, Officials Say," *The New York Times*, May 24, 2013, http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-from-iran-officials-say.html?_r=1&.

39 This article was written as nuclear negotiations were taking place between Iran and the great powers. One cannot rule out the possibility of escalating energy sanctions should the negotiations fail.

40 Siobhan Gorman and Danny Yadron, "Iran Hacks Energy Firms, U.S. Says," *The Wall Street Journal*, May 23, 2013, http://online.wsj.com/news/articles/SB10001424127887323336104578501601108021968.

41 Chris Strohm, "Iran-Based Hackers Traced to Cyber Attack on U.S. Company," *Bloomberg News*, May 14, 2013, http://www.businessweek.com/news/2013-05-14/iran-based-hackers-traced-to-cyber-attack-on-company-inside-u-dot-s-dot.

42 Shanker and Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers."

43 Barnes and Gorman, "U.S. Says Iran Hacked Navy Computers."

44 Gili Cohen, "Netanyahu Confirms: U.S. is Working with Israel on Cyber Defence, Iranian Attacks Increasing," *Ha'aretz*, June 9, 2013, http://www.haaretz.com/news/diplomacy-defense/.premium-1.528728.

45 "Israel's Aviation Agency under Muslim Hackers' Control for Months," *Fars News*, January 8, 2013, http://english.farsnews.com/newstext.aspx?nn=13921018001457.

46 "Saudi Army, Al-Qaeda Company, Israeli Army Hacked in Revenge for Assassination of Hezbollah Leader," *Fars News*, December 16, 2013, http://english.farsnews.com/newstext.aspx?nn=13920925001699.

47 Damien McElroy and Ahmad Vahdat, "Iranian Cyber Warfare Commander Shot Dead in Suspected Assassination," *The Telegraph*, October 2, 2013, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html; Lisa Daftari, "Internal Plot, not Israel, Eyed in Latest Hit on Iranian Scientist," *Fox News*, October 8, 2013, http://www.foxnews.com/world/2013/10/08/internal-intrigue-not-israel-eyed-in-latest-hit-on-iranian-scientist.

48 Simon Tisdall, "Iran Helping Syrian Regime Crack Down on Protesters, Say Diplomats," *The Guardian*, May 9, 2011, http://www.theguardian.com/world/2011/may/08/iran-helping-syrian-regime-protesters; Lisa Daftari, "Iranian General Admits 'Fighting Every Aspect of a War' in Defending Syria's Assad," *Fox News*, August 28, 2012, http://www.foxnews.com/world/2012/08/28/iranian-general-admits-fighting-every-aspect-war-in-

defending-syria-assad; Geneive Abdo, "How Iran Keeps Assad in Power in Syria, "*Foreign Affairs*, August 25, 2011, http://www.foreignaffairs.com/articles/68230/geneive-abdo/how-iran-keeps-assad-in-power-in-syria.

49 Ronald Deibert, "Waging the Cyber War in Syria," *National Post*, May 21, 2013, http://fullcomment.nationalpost.com/2013/05/21/ronald-deibert-waging-the-cyber-war-in-syria.

50 Joseph Menn, "Syria, Aided by Iran, Could Strike Back at U.S. in Cyberspace," *Reuters*, August 29, 2013, www.reuters.com/article/2013/08/29/us-syria-crisis-cyberspace-analysis-idUSBRE97S04Z20130829.

51 Sarah Hurtubise, "Syrian Hacker Army Could be Advancing with Iranian Help," *The Daily Caller*, April 9, 2013, http://dailycaller.com/2013/09/04/syrian-hacker-army-could-be-advancing-with-iranian-help; Andrea Peterson, "The Post Just Got Hacked by the Syrian Electronic Army. Here's who they are," *The Washington Post*, August 15, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/15/the-post-just-got-hacked-by-the-syrian-electronic-army-heres-who-they-are.

52 Kenneth Geers and Ayed Alqartah, "Syrian Electronic Army Hacks Major Communications Websites," *FireEye*, July 30, 2013, http://www.fireeye.com/blog/technical/cyber-exploits/2013/07/syrian-electronic-army-hacks-major-communications-websites.html.

53 "Syrian Electronic Army Reveals Documents of Haifa Hack," *Fars News*, June 15, 2013, http://english2.farsnews.com/newstext.php?nn=9203180050.

54 Elad Salomons, "Did the Syrian Electronic Army Attack Haifa's Water Supply SCADA System?" *Water Simulation*, June 5, 2013, http://www.water-simulation.com/wsp/2013/06/05/did-the-syrian-electronic-army-attack-haifas-water-supply-scada-system.

55 Menn, "Syria, Aided by Iran, could Strike back at U.S. in Cyberspace."

56 Olivia Goldhill and Reuters, "Benjamin Netanyahu: Iranian Cyber Attacks on Israel 'Non-Stop,'" *The Telegraph*, June 10, 2013, http://www.telegraph.co.uk/technology/10110381/Benjamin-Netanyahu-Iranian-cyber-attacks-on-Israel-non-stop.html.

57 "Terrorism in Cyberspace: Hezbollah's Internet Network," *The Meir Amit Intelligence and Terrorism Information Center*, March 4th, 2013, http://www.terrorism-info.org.il/en/article/20488.

58 David E. Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks," *The New York Times*, February 24, 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?hp&_r=2.

59 Amos Harel and Gili Cohen, "2014: Iran out, Global Jihad in," *Haaretz*, February 1, 2014, http://d26e8pvoto2x3r.cloudfront.net/uploadimages/systemfiles/iran%20out,%20global%20jihad%20in.pdf.

Call for Papers

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

Articles may relate to the following issues:

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

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

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