Military and Strategic Affairs

Volume 7 | No. 1 | March 2015

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 7 | No. 1 | **March 2015**

CONTENTS

Military and Strategic Affairs

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

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

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

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

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

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

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

Helicopters against Guerrilla and Terrorism: The Uniqueness of the Israeli Model

Tal Tovy

This essay discusses the role of the IDF's fighter helicopters in Israel's ongoing war against non-state actors. The essay first discusses the theoretical aspect of deploying aerial forces in a war against non-state actors and the advantages inherent in attack helicopters. The second part of the essay analyses the use of helicopters in armies around the world in this type of warfare, highlighting the IDF's unique modus operandi, which is discussed in the third part of the essay. The essay's conclusion is that the IDF does not view attack helicopters as a stand-alone weapons system but rather as another means by which it achieves its operational objective. Many operations undertaken by helicopters can be effected by other forces, but the use of helicopters attains a similar effect at lower risk. Furthermore, helicopters showcase Israel's technological and operational superiority, which may also result in an effect on public opinion, an aspect of great importance in warfare against non-state actors.

Keywords: attack helicopters, terrorism, guerrilla, non-state actors, the Israeli air force, IDF

Introduction

Israel has endured blood-soaked battles against non-state actors, starting almost immediately after the War of Independence in 1948. The IDF has used – and continues to use – a range of methods to provide maximum security for the citizens of the state. Among these actions, one may point to special operations and elite unit missions against terrorists' basecamps,

Dr. Tal Tovy is an Assistant Professor at the History Department, Bar Ilan University, Israel.

routine security activity along the borders, and targeted assassinations of terrorist leaders and dispatchers deep in the heart of the enemy's nations and even on European soil.

Occasionally, the IDF carries out extensive operations in an attempt to damage terrorist infrastructures (Operation Qarame, purging "Fatahland," Operations Litani, Grapes of Wrath, Protective Shield, Cast Lead, and Protective Edge, among many others). One could say that in its first months, Operation Peace for Galilee (1982) was the largest purging operation the IDF has ever undertaken. While the IDF's ground forces usually lead the war on terrorism and guerrilla forces,[1] since the Six-Day War the IDF has been increasingly relying on the Air Force to supplement its ground operations.

This essay discusses the function of the IDF's attack helicopter array in the ongoing war against non-state actors. It comprises a description of Israel's counter-terrorism and counter-guerrilla efforts with the use of attack helicopters as a test case. The essay has two further subsections: the first examines the theory of deploying helicopters against non-state actors, while the second briefly examines the use of helicopters by other armies in their respective counter-guerrilla warfare. The purpose of the latter section is to construct the historical operational framework that highlights the uniqueness of the IDF's use of attack helicopters. The essay's general aim is to highlight the unique use made of attack helicopters by the IDF, as the use of attack helicopters since the outbreak of the Second Intifada at the end of 2000 was not self-evident; as commander of the Apache helicopter fleet stated in a 2002 interview: "Two years ago [September 2000] nobody thought attack helicopters would be used in this type of warfare."[2]

Air Force and Warfare against Non-State Actors: Theoretical Framework

In every military confrontation – including against non-state actors– there is tactical and strategic tension between defense and offense and between standoff fire and the ground maneuver.[3] The IDF's principles of warfare stress offense as "the most effective way of seizing the initiative" and "whoever seizes the initiative dictates the fighting and imposes his will on the enemy."[4] Compared to combat against regular forces, achieving victory in warfare against non-state actors is much more complex because it cannot be attained by a one-time action; furthermore, political constraints impede decision-making processes while in regular warfare, there is exclusive importance to the military efforts and the combat moves of the

various army units (although the distinction is growing fainter), in warfare against non-state actors, the patterns of activity are different. Non-state actors usually enjoy widespread support among the local population as well as excellent knowledge of the geographical conditions in which they operate. It is therefore necessary to create the right mixture of political, economic and social action to improve the standard of living of the civilian population, thus undermining the popular support that is so important to guerrilla fighters.

While military activity should not be over-emphasized, it remains a critical component of warfare. The military modus operandi is to eliminate belligerent non-state actors through exhaustion, attrition, and weakening of guerrilla forces, with the main objective being to prevent losses and minimize attrition on their side. Furthermore, the regular army must bring its technological superiority to bear on the fighting. The essay asserts that, from the military aspect, the attack helicopter is the ideal platform for fighting guerrilla. The deployment of the air force in general, and attack helicopters in particular, serves several goals representing the theoretical military foundation for warfare against non-state actors.[5]

One of the prominent features of fighting guerrilla forces is the inherent asymmetry, i.e., the imbalance and inequality between the sides. The IDF has clear and absolute technological superiority, manifested in the use of an air force and other army branches. This technological superiority also helped other nations fighting guerrilla forces (discussed below). A nation fighting guerrilla forces and/or terrorists is not required to justify the leveraging of its technological superiority, though it is critical to avoid harming civilian non-combatants. Aerial forces provide a regular army with flexibility, mobility, firepower, maneuvering and real time combat intelligence. In Israel, such aerial forces consist of Sa'ar helicopters to transport special forces, fighter jets for forceful attacks on any given location at any given time, UAVs to gather intelligence, airborne communications systems (currently also equipped with weapons), and, of course, attack helicopters.[6]

Attack helicopters have several prominent advantages. First, their mobility is not affected by terrain, and they have the capacity to operate in long ranges compared to ground forces. The second advantage is the ability to deploy force at short notice. An attack helicopter task force can be placed in relatively well protected bases, unlike ground-based task forces. In many battles against guerrilla forces, the conquest of territory

is pointless. Moreover, territory that is captured and held by infantry and armored forces has always been the preferred target for attack by guerrilla fighters, and they also result in operational and logistical difficulties for a regular army. For example, most of the IDF's losses throughout its presence in Lebanon (1985-2000) occurred not as a result of proactive operations but as a result of logistics: opening routes, moving supply convoys, and securing the outposts.[7] When the IDF seized the initiative, its high operational capabilities in tandem with technological and firepower superiority were manifest. A significant portion of proactive operations was carried out by attack helicopters.

Another advantage inherent in attack helicopters is the range of precision arms they can carry as well as their firepower at extended ranges, i.e., mobility combined with firepower. Attack helicopters can accompany helicopters ferrying ground-based task forces to special operations while providing nearby air support and cover for landing and evacuation from the area of action. The final advantage is the attack helicopters' versatility. Guerrilla warfare is characterized by non-frontal fighting, and guerrilla forces can attack anywhere at any time. It is impossible to maintain masses of ground forces everywhere at all times, because it is very difficult to predict where and when the guerrilla forces might attack. By contrast, attack helicopters can quickly reach any arena of activity and provide the required firepower. If a shooting incident lasts a long time, Sa'ar helicopters can ferry infantry troops to the scene of fighting. This is in fact the primary function of the attack helicopter; attacking the enemy's infiltration attempts in those locations where the defensive systems are liable to collapse or where they don't exist in the first place.

To the gamut of these qualitative and quantitative advantages we should add an advantage that is difficult to quantify. As aforementioned, guerrilla warfare is characterized by its asymmetry. The use of aerial forces presents the qualitative and technological advantage of the "strong," thereby forming a kind of basis for psychological warfare. If the use of aerial forces is precise and causes serious damage to the human and logistical infrastructures of the side employing guerilla tactics, the aerial forces serve as an important method of negating the guerrillas' belief that they can win.[8] The ability to strike from a distance with the element of surprise and retreat unharmed also contributes to the physical and psychological undermining of guerrilla forces. Based on testimony gathered by the human rights organization B'tselem, it appears that many eyewitnesses specified the fact that they

were unable to pinpoint where the fire had originated and that the initial burst of fire had been sudden, quick, and fatal.[9] These points (without entering a moral debate about Israel's modus operandi) demonstrate the attack helicopters' advantages in harming the human infrastructures of terrorist organizations. One should note that, based on foreign sources, some of the more recent targeted assassinations have been carried out by unmanned aerial vehicles.

At the same time, helicopters have several drawbacks. The main disadvantage lies in the fact that this very sophisticated and expensive platform is vulnerable to attack by simple, cheap arms. A helicopter flying at low height is exposed to anti-aircraft fire, such as cannons, machine guns, and shoulder mounted rocket launchers. Thus, for example, two U.S. Special Forces Black Hawk helicopters (of the UH-60 model) were downed by an RPG-7 in Mogadishu, Somalia, on October 3, 1993. The vulnerability of attack helicopters was also evident during U.S. operations in Afghanistan and Iraq. Another drawback is the difficulty of operating attack helicopters in tough weather conditions. Visibility (nighttime, fog, etc.) limits their use as well, though this factor is gradually being mitigated by advanced night vision systems.

Despite their vulnerability, the nature of a helicopter's warfare system allows it to launch guided missiles from long distances, thereby surprising guerrilla forces. By the time they manage to regroup, the helicopter can be long gone from the fire zone. The Apache's "fire-and-forget" ability is an excellent example of a regular army's ability to use its technological superiority against guerrilla forces. The combination of great mobility, short response times and the concentration of heavy firepower makes attack helicopters an effective, lethal weapon system in confronting guerrilla forces and/or terrorists.[10] In addition, the helicopters' effectiveness comes to the fore due to the fact numerous confrontations in the last few decades have taken place in densely populated urban settings, requiring the ability to cause pinpoint damage so as to minimize casualties among non-combatant civilians. Attack helicopters as a weapons system thus incorporate technologies supporting operational needs as well as the desire to reduce the number of casualties to the civilian population.[11]

Similar advantages may be found in the increased use of unmanned aerial vehicles in the day-to-day fight against non-state actors. In November 2001, a U.S. report noted that a UAV had carried out an attack in Afghanistan, the first documented use of a UAV carrying out an attack and going beyond

the traditional missions of patrol, observation, intelligence gathering, and marking targets. While many foreign sources identify Israel as being the first to use UAVs in military operations, the first reliable report of UAVs deployed in an attack mission appeared in the press only on October 24, 2004, when an eyewitness reported an attack in Khan Younis. Reports on attacks by "Israeli aerial vehicles" continued to appear in subsequent years. In fact, Israel is identified as one of only three nations – in addition to the United States and Great Britain – using UAVs in attack missions against various targets. However, because Israel has never officially declared that it uses UAVs in attacks in Gaza, southern Lebanon, and other locations, the United States is considered the first to do so.[12] This essay therefore focuses on the unique use Israel makes in proactive attacks on non-state actors, a uniqueness resulting in two processes, the first being the fact that the Israeli method – using attack helicopters as a weapons system in fighting non-state actors – has been adopted by other nations, and the second being the addition of combat missions to UAVs aside from their traditional use as a platform for patrolling and intelligence gathering. To examine the IDF's unique use of helicopters in general and attack helicopters in particular (more on this below), it is first necessary to examine the use made of helicopters by other armies that have confronted non-state actors.

Historical Experience: Helicopters Used against Non-State Actors in Armies around the World

France: Indochina and Algeria

In the aftermath of World War II, France tried to reconstruct its empire through two long and difficult campaigns; Indochina in 1946-1954 and Algeria in 1954-1962. In Indochina, the French army used helicopters mostly in rescue and evacuation operations.[13] The use of helicopters began in 1950, and French helicopters were used much like U.S. helicopters were used in the Korean War. France had plans to transport infantry using helicopters but these were never put into effect because of the defeat suffered at Dien Bien Phu, which ended the war.

During the Algerian campaign, helicopters began playing a more significant role.[14] The new missions included transporting troops to the battlefields based on operational needs and achieving a quantitative and qualitative advantage at any given place and time. Algeria's enormous size, consisting mostly of desert terrain, posed strategic, operational,

tactical, and logistical problems for the French, while the topography greatly helped the Algerian guerrilla fighters. The operational solution was massive use of helicopters. When a guerrilla unit was identified, elite French troops were quickly brought in to engage in pursuit, while other units established roadblocks and prepared ambushes along the guerrillas' path. If the pursuit lasted for many hours, helicopters were used to bring in supplies, ammunition, and new manpower.[15]

Great Britain: Malaya

Great Britain confronted a long series of guerrilla wars following World War II as well. The longest and most intensive campaign was in Malaya in 1948-1960. The primary British innovation lay in the manner in which it handled landing and collecting troops for patrol missions and, later on, in areas where guerrilla units were expected to operate. The first mission was carried out in February 1952 and consisted of evacuating infantry troops cut off because of flooding.[16] Later on in the war, helicopters continued to transport and evacuate troops, sparing forces the need to advance through Malaya's difficult terrain of mountainous jungles.[17] In addition, helicopters have served in their classical roles of evacuating the wounded and bringing supplies to isolated outposts.

The United States: Vietnam – the Helicopter War[18]

The primary feature of the Vietnam War was the United States' massive use of helicopters, to the extent that they became, with good reason, one of the war's most widely recognized emblems. The second innovation was turning helicopters into platforms carrying various types of arms for use in close aerial assistance tasks. The transport of large numbers of troops across long distances in a short amount of time was not the result of a new anti-guerrilla doctrine of warfare, but was rather a notion that had been developed prior to the U.S. involvement in Vietnam for a scenario involving a limited nuclear war in Europe.[19] It gradually emerged that the high mobility afforded by helicopters could provide an effective response to the mobility of the guerrillas and the challenges posed by Vietnam's topography and climate.

The first U.S. helicopters arrived in Vietnam in late 1961 and began flying combat missions as part of the South Vietnamese Army, though very quickly they were flown by U.S. pilots who shared their experience to draw lessons for future operations. The main lesson learned was that every

helicopter transporting troops should be accompanied by 5-7 gunships, i.e. helicopters armed with machine guns, grenade and rocket launchers in order to protect the troops in the "slick" upon deployment on ground. To complete the combat structure, helicopters would be included for rapid evacuation of the wounded and there would be a command and control helicopter to coordinate the whole landing operation. The doctrine of deploying such formations earned the name Eagle Flight.[20]

As the U.S. involvement in the ground fighting in Vietnam expanded during 1965, the U.S. Army began deploying paratroopers and infantry forces via helicopters. These divisions, like the 101st Airborne and the 1st Cavalry, were merged with helicopter squadrons similar to artillery and engineering troops. Gradually, helicopters were incorporated into all Army and Marines combat units operating in Vietnam. The numbers speak for themselves: during the war, up to the final evacuation of U.S. troops from South Vietnam in the first half of 1973, U.S. helicopters carried out some 36,125,000 missions. Of these, some 3,932,000 were attack missions; 7,547,000 were for inserting troops; 3,548,000 were logistical in nature; and more than 21,000,000 missions were designated for patrols, evacuating wounded, extracting pilots, and other tasks. The United States lost 2,066 helicopters to enemy fire and 2,566 under other circumstances.[21]

The doctrine of warfare developed during the 1960s included the massive use of helicopters to locate the enemy, insert troops to eliminate guerrilla insurgents, provide ground forces with close aerial support, or move artillery to new positions. On the logistics level, helicopters served as platforms for command and control, communications, transporting supplies to the fighting troops, and evacuating the wounded. Massive use of helicopters and the existence of helicopter units as organic components of the divisions and independent brigades resulted in the U.S. Army being capable of transferring units quickly over great distances, and bringing them a steady flow of supplies as well as providing combat support.

During the Vietnam War, specially designated attack helicopters of the AH-1G Cobra model were introduced into operational combat use.[22] The Cobras were quicker and better able to maneuver than previous models. Towards the end of the war, armed helicopters of the Bell UH-1 model were still in use to provide proximate air cover to infantry fighting on the ground. During the war and thereafter, the United States continued to upgrade its helicopters' combat capabilities. This process peaked with the 1984 introduction of the AH-64 Apache into active service. While this

helicopter was developed on the basis of the lessons learned in Vietnam, its main objective quickly turned into a platform to help block masses of Warsaw Pact armored vehicles as part of the Air-Land Battle doctrine developed in the 1980s. In other words, the new attack helicopter was defined as having functions in regular wars as part of the United States' new conceptual framework that formed the basis of its army's European warfighting doctrine in the post-Vietnam era.

At present, helicopters of various types are an inseparable part of the U.S. Army's formations in every possible outline. In the 40 years since the end of the Vietnam War, helicopters have had an important – sometimes decisive – role in the various military activities. In addition to moving an entire brigade from the 101st Airborne during the ground invasion in the Gulf War[23] deep into the heart of the Iraqi army, helicopters played an important role in military interventions in low intensity confrontations such as Granada (1983), Panama (1989), Somalia (1983), Afghanistan, and Iraq. In the Second Iraq War the use of attack helicopters was problematic and exposed the helicopters' weaknesses in environments where there is no clear demarcation between friendly and enemy troops.

The USSR/Russia: Afghanistan and Chechnya

The USSR's most important official experience in fighting against guerrilla forces across its own borders was in Afghanistan. The use of Soviet helicopters during many types of operations did not represent any tactical or operational innovation, especially after Vietnam. Nonetheless, when reading the literature about the use of helicopters in Afghanistan, it seems that the U.S. experience was ignored by the Soviets who stumbled from one approach to another in an attempt to find the right tactic for helicopter deployment. As the war dragged on, the Soviets engaged in increasingly daring operations until the summer of 1986, when the Western-sourced Blowpipe and Stingray anti-aircraft missiles came on the scene. Unlike the United States, the Soviet Union reduced the scope of helicopter activity once this threat emerged. While the extent to which the Mujahidin were able to operate the anti-aircraft weapons is unclear, the USSR was not prepared to suffer the casualties caused by advanced missiles. Western assessments determined that most of the Soviet helicopters downed in Afghanistan were actually hit by sub-machinegun fire and RPG rockets. The Somali militias who downed the U.S. helicopters in Mogadishu, for example, were trained by such fighters.[24] Still, it should be noted that the

reduction in the use of helicopters by the Russians also stemmed from a political decision to scale back the Soviet presence in Afghanistan.

The first helicopters in Afghanistan were apparently deployed in the last third of 1980. In September and November of that year, the USSR carried out two large operations to clear out the Mujahidin from the Panjshir Valley. Troops were brought in by helicopter to land in position of controlling terrain in tandem with the advance of ground forces. The goal was to block the Mujahidin's retreat routes from the valley to the mountains and engage them in battle in conditions that were advantageous to the Soviet forces. From the second half of 1981, the insertion of troops into strategic areas along the axes of the advancing ground troops became an integral part of Soviet tactics. The use of helicoptered troops became more aggressive and incorporated proactive steps, such as going out on missions to discover the guerrillas' hiding spots.

During 1982, the Soviets adopted the search-and-destroy tactic used by the United States in Vietnam. The introduction of the Mi-24 Hind and Mi-28 Havoc models into action allowed operations outside the fire-scope of the Soviet artillery. Proximate aerial support from attack helicopters became a key component in the Soviet forces' overall firepower. Gradually, the ratio between the mechanized forces and the helicopters changed in favor of the latter.[25] In tandem with the combat duties of landing fighters, providing proximate air support, and serving as "flying artillery," the helicopters were also deployed to provide armed escort to supply convoys and bring supplies to positions that were either very distant or whose ground access was deemed dangerous.

In December 1994, Russia began its large-scale involvement in Chechnya. There, as in Afghanistan, the Russians fought guerrilla units enjoying the advantages of mountainous topography. One may have expected that the lessons learned a decade earlier would have been turned into an orderly military doctrine. But the weakness of the Russian economy affected the army's fitness and capabilities. The main tasks of the helicopters in Chechnya were logistical: bringing supplies to the fighting units and evacuating the wounded (44 percent of all missions). The combat missions mostly involved escorting convoys and landing troops.[26] Still, some combat missions were carried out in which the attack helicopters' firepower was demonstrated.

Summary of Other Armies' Operational Experience with Helicopters

Generally speaking, one can summarize the operational experience of other armies by saying that the use of helicopters replaced operational paratroopers. Inserting troops via helicopter is faster and more precise: as techniques for landing troops developed, the number of losses dropped in comparison with operational parachute jumps, especially in areas where one could expect the enemy to effectively fire surface-to-air weapons at the paratroopers.[27] The following is a list of functions in their order of development:

1. Logistical tasks, including evacuation of wounded and retrieval of pilots.
2. Observation, intelligence gathering, and command and control tasks.
3. Troop insertion.
4. Proximate air support for convoys and ground troops.
5. Independent combat missions against guerrilla targets.

The Use of Combat Helicopters in the IDF (from 1979)

The creation of the IDF's helicopter structure can be divided into two major stages. The first stage began when helicopters were first integrated into the Air Force in May 1951 and lasted until 1975. At that time, the helicopters' main function was to undertake observations, gather intelligence, fly in commanders, and bring forces to and from the battlefield. In other words, the IDF deployed its helicopters similarly to the way other armies around the world did.[28]

The second stage began after the lessons of the Yom Kippur War had been studied. The Israeli air force suffered terrible losses because of the dense, aggressive anti-aircraft fire directed at it, so that it was unable to stop the masses of Syrian and Egyptian armored corps or help Israel's infantry and armored units. After the war, the IDF decided to acquire attack helicopters to be better equipped in the future to handle masses of armored vehicles attacking in an area saturated with anti-aircraft systems. But such missions were never carried out; in fact, one may say that after the Yom Kippur War and the continued fighting against Syria in the following months, the IDF did not confront regular Arab forces again. The exceptions to this were the battles against the Syrian army during the First Lebanon War. Given that the United States had been Israel's major arms provider, including fighter planes, since the late 1960s it was only natural that Israel's future helicopter acquisitions would be from the United States. The introduction

of the Cobra AH-1Q helicopter into service in April 1975 and the completion of the attack helicopter structure with the Defender MD-500 model mark the second stage of the creation of the IDF helicopter formation. During the 1990s, the advanced Apache attack helicopters were added.

In Operation Litani (March 15-21, 1976), the helicopters were not yet used to attack, the main reason being that the Cobras were having their weapons systems upgraded. It was only at the end of the 1970s that the IDF's attack helicopters began operating in Lebanon. Their main function was to fire missiles and other munitions at the various terrorist organizations' ground targets. In practice, these helicopters demonstrated excellent, accurate operational ability in attacking ground targets. The use of attack helicopters significantly reduced harm to civilian targets, which had been difficult to prevent when fighter planes were used.

The Cobra helicopters' first operational activity took place on May 9, 1979, when two helicopters attacked a building near Tyre where terrorists were hiding.[29] Defender helicopters began their operational activity in Lebanon about a year later. Combat helicopters operated during the initial stages of Operation Peace for Galilee against regular Syrian army forces, damaging their tanks and other armored vehicles.[30] The Lebanon War incorporated elements of conventional warfare with anti-guerrilla fighting, thus manifesting the operational flexibility provided by attack helicopters. But to this point the IDF's use of helicopters entailed no real innovation.

The importance of the attack helicopter was discovered during the prolonged war against Hizbollah. The IDF incorporated the airborne structure in southern Lebanon, with one of the main tools being the attack helicopter. In addition, upon eruption of the Second Intifada in the West Bank and Gaza Strip (September 2000), attack helicopters played an important role in the Israeli response. The attack helicopters' operations and missions in the West Bank and Gaza Strip were similar to those carried out in southern Lebanon. There is no doubt that the use of attack helicopters highlighted the IDF's military and technological might in the anti-terror campaign. In addition, attack helicopters, when used to provide proximate aerial support, reduced the number of infantry casualties.

The scope of missions carried out by attack helicopters in Lebanon were a manifestation of their inherent operational capabilities. In Lebanon, the IDF encountered two major problems: the first, infantry and armored units were caught in Hizbollah ambushes; the second was the IDF's attempt to identify and destroy the Katyusha launchers that were shelling northern

Israel, a difficult and frustrating task. The attempt to identify the launchers required real-time intelligence, attained by UAVs and other intelligence tools. The moment a Katyusha launcher was identified attack helicopters (or the artillery) were called in to strike at the launcher and its operators. Sometimes the launcher would be identified only after rockets had already been fired, at which point the objective was to disarm and prevent further use.

The arrival of the Apache helicopter enhanced operational capabilities. The Apaches were delivered to the air force in September 1990 and shortly thereafter became part of the operational routine in Lebanon. The Apaches, with their advanced technological and armaments capabilities compared to other attack helicopters in the air force, generated the development of the method of targeted assassinations of senior members of terrorist organizations. These missions are discussed in this essay based on their operational use and merit, not their moral stature. On February 15, 1992, two Apache helicopters attacked a convoy transporting Hizbollah Secretary General Abbas Mussawi; on May 31, 1995, and on August 25, 1998, senior Hizbollah members were the focus of a targeted assassination. In general, one may say that Apache helicopters were deployed in every single scenario of routine operational activity in Lebanon, but especially in precision operations that required nighttime activity. The Apaches' high level of operational ability was again proven in Operation Accountability (July 1993) and Operation Grapes of Wrath (April 1996). The helicopters were deployed mostly in order to cause precision damage to terrorist targets.

Starting in September 2000, the Second Intifada in the West Bank and Gaza Strip proved the high operational capabilities of attack helicopters.[31] Use of the targeted assassination method intensified and dozens of terrorists were eliminated by attack helicopters at the end of complex intelligence gathering operations. Most of the terrorists killed were senior members of various terrorist organizations (Hamas, Islamic Jihad, and the Tanzim) who were responsible for many terrorist operations, including the dispatch of suicide bombers into Israeli cities. During 2001, attack helicopters carried out more than 65 attacks in all arenas and at all hours of the day and night.[32] Although fighter planes were also used, most of their missions involved the destruction of targets belonging to the Palestinian Authority and other organizations, such as command centers, munitions storage, and government structures. Upon introduction of pinpoint activities or when targets were located deep in the heart of civilian areas and there was concern that innocent civilians would be harmed, attack helicopters

became the tool of choice. Thus, for example, on July 31, 2001, Apache helicopters killed two senior Hamas commanders and four of their men.[33] It has often been claimed that these precision operations were carried out with close integration of helicopters and UAVs.

The attack helicopters' mission is to provide an aerial umbrella and proximate airborne assistance to ground forces as they engage in operational activities. The operations during the Second Intifada entailed difficult battles against guerrilla forces in densely populated urban centers. The urban terrain limits the infantry forces' mobility and observational capabilities.[34] To this extent, Apaches have many advantages: firepower of great intensity, concentration and precision, and observation capabilities, including thermal night visions systems (e.g., FLIR, the Forward Looking Infra-Red system). Connecting helicopters' operational components with the ground forces resulted in doubling the power of any unit operating in any delimited location.[35]

In the difficult, complex warfare against terrorists, attack helicopters earn maximal media exposure. In April 2002, a BBC report presented Israel's war on terrorism, including the targeted assassinations of terrorists by attack helicopters. The report implied that one of the ways to eliminate a wanted terrorist is by ambush. The report showed the classical method, i.e., ambush by infantry, as well as the innovation used by the IDF is the elimination of wanted terrorists by ambush by attack helicopter.[36]

Despite the drawbacks of using attack helicopters, especially their high cost, they do represent an offensive platform. Attack helicopters improved the IDF's offensive capabilities in guerrilla warfare and reduced the number of potential casualties in urban areas. The helicopters' daily activities resulted in constant pressure on the guerrilla units. Generally and historically speaking, one may say that the more the side confronting guerrilla warfare and/or terrorism engages in offensive strikes, the more the guerrillas are forced into defensive positions, thus resulting in a decrease of their attack capabilities.[37] It may be that a drop in operational capabilities will, to one extent or another, damage the guerrilla forces' ability to achieve their political ends.[38]

The uniqueness of the IDF's deployment of attack helicopters, as discussed herein, lies in using them in designated offensive missions while seizing the initiative in fighting against guerrillas and/or terrorists. In order to further highlight the Israeli uniqueness it is necessary to examine the

attack helicopter's function in the United States and Great Britain's fight against guerrillas and/or terrorists until 2001.

The literature dealing with Great Britain and the United States' Special Forces and counterterrorism units shows that the helicopters' primary function is to land masses of troops and provide proximate airborne support, i.e., the traditional roles of helicopters as developed in the 1950s. Other than some technological innovation (the introduction of more modern helicopter models), there has been no operational innovation in the deployment of attack helicopters in Western nations.[39]

There is no evidence that the British used attack helicopters against high-quality human targets of the Irish Republican Army. Unlike what is commonly thought, the war against the IRA took place not only in the large cities of Northern Ireland but also in rural settings. The war against the Irish underground saw the participation of the army, police and the 22nd Regiment of the Special Air Service.[40] Thus, for example, in May 1987, British intelligence learned of the IRA's intention to detonate a Royal Ulster Constabulary base using a car bomb. Although IRA members were under close surveillance, the British waited for the terrorists to come to the base, whereupon they were eliminated in an ambush set by the SAS team. The base was destroyed in the explosion; civilians who were in the church next-door were exposed to real danger.[41] It is not at all clear why the IRA operatives were not eliminated on their way to the Royal Ulster Constabulary base located in the village of Loughgall, deep in the heart of farm country. Because the intelligence was reliable and precise, it would have been possible to destroy the vehicle driven by the terrorists by attack helicopter. It is worth noting that when the attack on the base began, an SA-341 Gazelle helicopter was called in to patrol the area to identify further suspects and steer the army forces towards them, but this was a patrol and observation mission rather than a combat mission.

Similarly, the "FM 7-98: Operations in a Low Intensity Conflict," a U.S. Army field guide, devotes only a single, brief paragraph to the deployment of attack helicopters in operations involving low intensity warfare. Although the paragraph begins by saying "attack helicopters are a highly mobile and immediate-response maneuver element,"[42] afterward it mostly refers to operational activity involving missions such as security, supply convoy escort, patrol and proximate airborne assistance to ground forces. In other words, the attack helicopter is treated primarily as a platform for providing assistance. The main point of the guide's seventh chapter is

combat assistance, such as artillery of various kinds, anti-tank fire, tactical air support (fixed-wing planes), and fire assistance from naval platforms. In the U.S. doctrine, the attack helicopter in the context of low intensity warfare is viewed as an auxiliary weapon, without being defined as a weapons system seizing the offensive initiative.

Conclusion

Israel's war against non-state actors is a daily, ongoing affair. The essay attempted to point to the unique offensive activities that the IDF has made and continues to make with the help of attack helicopters, an operational model that has been adopted by other nations, especially the United States as it became entangled in fighting against non-state actors in Afghanistan and Iraq. The IDF never viewed the deployment of the helicopter as a stand-alone method, but always as an additional tool to attain an operational result. Many actions carried out by helicopter can be handled by other forces, but its use achieves a similar effect at lower risk. Furthermore, helicopters symbolize Israel's technological and operational superiority, so it is also possible they have a psychological impact, an important aspect in fighting against non-state actors. It should be said that the Israeli air force is aware of the fact that the organizations it fights arm themselves with advanced anti-aircraft weapons so that the helicopter is now more vulnerable than it was in the past. This may increase the use of UAVs, also because the unmanned platforms can remain in the air longer than helicopters can.

Nonetheless, it is too early to eulogize the helicopter as an effective combat platform. The U.S. experience shows that despite the helicopter's vulnerability the platform can continue to operate. This is also true of Israel. The attack helicopter plays an important part in the IDF's offenses against irregular troops. Operation Protective Edge in the summer of 2014 demonstrated that, despite the increasing use of UAVs (based on foreign reports, attack helicopters continue to fulfill a significant function when fighting non-state actors. Such activity is characterized by the seizing of initiative and serves several goals: first, foiling terrorist attacks both by eliminating the terrorists on their way to the target and by assassinating the organizations' leaders; second, taking out leaders as an independent goal so as to disrupt the organizations' functioning. Here it is important to note that an exact, high-quality strike based on intelligence requires the organization to close ranks and examine how the information leaked out. The success of a targeted assassination makes organization leaders

conclude that they are not safe even among their own supporters, causing rigid compartmentalization, which damages the operational effectiveness of a terrorist organization, in addition to the hit taken by the planners. It is possible to disrupt the operational and organizational routines by attacking organizations in areas they consider safe; third, deterrence stemming from the striking capabilities shown in previous operations and also as an announcement that harm to civilians in the state will result in a response; this leads to the fourth goal: morale. This aspect has several dimensions, though the most important would be damaging the morale of the enemy organization and its supporters and raising the morale of the citizens of the state.

The attack helicopter structure and its supporting structures, especially intelligence, facilitate the IDF's success in taking proactive offensive measures critical in wars against guerrillas and/or terrorists. The nature of attack helicopters has made them into a highly important warfare platform. Offensive proactivity shows terrorist organizations and their supporters, both passive and active, that the party fighting them is not defending itself and cowering while waiting for the next terrorist attack, but is taking practical steps and forcing the other side to seek cover.

The uniqueness of the use of the attack helicopter in fighting non-state actors in the West Bank and Gaza Strip (and earlier also in Lebanon) stems from its advantages, which include flexibility of operation, high firepower and precision strikes. In many cases, the weapons systems and munitions they carry allow attack helicopters to cause great damage to the specific target without harming the civilian surroundings. Such deployment was unique to the Israeli air force and until 2001 was not to be found in other nations fighting against irregular troops. Attack helicopters can maintain a sequence of activities without suffering attrition, can rapidly reroute the effort from one sector to another, and can execute precision strikes of selected targets. Nonetheless, every future action must take moral elements into account. To the extent that ground conditions allow it, one must always strive to avoid harming civilians. It is also necessary to weigh the damage wrought to any given terrorist organization against the damage to Israel's image should innocent civilians suffer harm.

Notes

1 Gunther E. Rothenberg, "Israeli Defense Forces and Low Intensity Operations," in *Armies in Low-Intensity Conflict*, D. A. Chaters and M. Tugwell, eds. (London: Brassey's Defense Publishers, 1989), pp. 49-72.

2 Israel Defense Forces, *The Air Force Bulletin*, August 2002, p. 6.

3 Christopher Bellamy, *The Evolution of Modern Land Warfare: Theory and Practice* (London: Routledge, 1990), pp. 15-17.

4 IDF General Staff-3-Sub-02, Operations Division, Doctrine and Training Section, *The Principles of Warfare*, 21 (2007).

5 For a general overview of the use of aerial forces against guerrilla forces see: Shmuel Gordon, *The Last Order of Knights: Modern Aerial Strategy* (Tel Aviv: Ramot, 1998), pp. 316-34; Ilan Hershkovitz, "The Aerial Component in Low Intensity Fighting," *Ma'arakhot* No. 380-381 (2001): 68-71. Both studies include a general discussion of the use of aerial forces in fighting against guerrillas; the ideas on the use of helicopters are derived from the studies without specific discussion of them. Nonetheless, Hershkovitz's study discusses different aspects of using aerial forces in the current confrontation with the Palestinians. Also see: Zaki Shalom and Yoaz Hendel, *Let the IDF Win: The Self-Fulfilling Slogan* (Tel Aviv: Yediot Aharonot Press, 2010), pp. 63-67.

6 Shmuel Gordon, *The Vulture and the Snake: Counter-Guerrilla Air Warfare: The War in Southern Lebanon* (Ramat Gan: Begin-Sadat Center for Strategic Studies, Bar-Ilan University, 1998), pp. 38-39.

7 The most extreme and tragic example is the infamous helicopter disaster of February 4, 1997, when two Yasur helicopters carrying soldiers to Lebanon collided mid-air. The soldiers killed were not on their way to engage in combat but merely sent to replace their comrades. All 73 men aboard the helicopters – soldiers and pilots – were killed.

8 Hershkovitz, "The Aerial Component in Low Intensity Fighting," p. 69.

9 B'tselem, *Position Paper: Israel's Assassination Policy: Execution without Trial* (January 2001): 3-4. I would like to stress that this study is in no way interested in discussing any political or ethical aspect of any war or confrontation.

10 Despite its intensive use in the West Bank, the Israeli air force has not forgotten the attack helicopter's basic function: attacking and eliminating armored vehicles in case of attack on Israel.

11 In this context, see: Isaac Ben-Israel, "The Use of Weapons in Densely Populated Areas," *Military and Strategic Affairs* No. 5, special issue (2014): 15-18.

12 It should be noted that the first U.S. attacks using UAVs were carried out by the CIA rather than the military. See: Thomas G. Mahnken, *Technology and the American Way of War since 1945* (New York: Columbia UP, 2008), pp. 201-202.

13 Bernard B. Fall, *Street Without Joy* (London: Stackpole Military History Series, 1961), p. 265; V.J. Croizat (tr.), *A Translation from the French Lessons of the War in Indochina,* May 1967 CORDS Information Library RG 472 (Records of the United States Forces in Southeast Asia, 1950-1975) box 19, file no. 101223, pp. 299-305.
14 Robert B. Asprey, *War in the Shadows: The Guerrilla in History* (New York: Doubleday, 1994), p. 676.
15 Hilaire Bethouart, "Combat Helicopters in Algeria," in *The Guerrilla and How to Fight Him*, T. N. Greene, ed. (New York: Praeger, 1966), pp. 260-69.
16 Robert Jackson, *The Malayan Emergency* (London: Routledge, 1991), pp. 98-102.
17 E.D. Smith, *Malaya and Borneo* (London: Allan, 1985), p. 35; Jackson, *The Malayan Emergency*, pp. 97-98.
18 The most comprehensive overview of the use of helicopters during the Vietnam War may be found in a study published by the Army Department as part of the series *Vietnam Studies*, published starting in 1973. See: J. Tolson, *Airmobility, 1961-1971* (Washington D.C., 1989).
19 Andrew F. Krepinevich, *The Army and Vietnam* (Baltimore: JHU Press, 1986), p. 112.
20 Ibid., pp. 38-39.
21 Spencer. C. Tucker, *Vietnam* (Lexington: University of Kentucky Press, 1999), p. 122.
22 Tolson, *Airmobility*, pp. 144-46.
23 Harry G. Summers, *Persian Gulf Almanac* (New York: Facts on File, 1995), p. 208.
24 Mark Bowden, *Black Hawk Down: A Story of Modern War* (New York: Grove Press, 2000), p. 133.
25 Anthony H. Cordesman and Abraham R. Wagner, *The Lessons of Modern War (vol. 3): The Afghan and Falklands Conflicts* (London: Westview Press, 1990), pp. 192-205.
26 Timothy L. Thomas, "Air Operations in Low Intensity Conflict: The Case of Chechnya," in *Airpower Journal* (Winter 1997).
27 Robin Neillands, *In the Combat Zone: Special Forces since 1945* (New York: Questia, 1998), p. 54.
28 For a general overview of the use of helicopters during the War of Attrition, see: Haim Nadel, "Between the Two Wars 1967-1973," *Ma'arakhot* (2006), pp. 230-33. For more on the function of helicopters during the Yom Kippur War, see: Anthony H. Cordesman and Abraham R. Wagner, *The Lessons of Modern War (vol. 1): The Arab-Israeli Conflicts, 1973-1989* (London, Mansell Publishing, 1990), pp. 100-101.
29 Eliezer Cohen and Zvi Lavi, *The Sky's Not the Limit: The Story of the Israeli Air Force* (Tel Aviv: Ramot, 1990), pp. 625-26.
30 Cordesman and Wagner, *The Lessons of Modern War* (vol. 1), pp. 210-13.

31 In the first two years of the Second Intifada, the Apache helicopters carried out some 1,500 missions in the West Bank and Gaza Strip. *The Air Force Bulletin* (August, 2002): 6.
32 Israel Defense Forces, *The Air Force Bulletin* (December, 2001): 6.
33 Israel Defense Forces, *The Air Force Bulletin* (August, 2001): 7.
34 See Gal Hirsch's comparison of a fighting force in an urban setting to a ball moving in all dimensions, including underground. Gal Hirsch, "Fighting in the Urban Sphere," *Military and Strategic Affairs* No. 5, special issue (2014): 19. It is, of course, necessary to remember that such operational problems are not unique to the contemporary urban setting but have already been a feature of complex fighting in constructed areas. The complexity lies in the fact that the urban environment contains non-combatants and international law does not tolerate harm befalling them.
35 Israel Defense Forces, *The Air Force Bulletin* (April 2002): 38.
36 *Jane's Defence Weekly*, January 9, 2001.
37 The tension between routine security entailing many casualties and offensive initiative comes to the fore in Moshe Tamir's book about the years Israel maintained a presence in southern Lebanon. See: Moshe Tamir, *War Without a Sign* (Tel Aviv: Ramot, 2006). Thus, for example, on p. 127, he describes the ambush of an IDF convoy in which three Israeli soldiers were killed. On the same page, he also mentions the Egoz Unit's seizing of the initiative, thanks to which two Hizbollah operatives, who were apparently involved in preparing the ambush, were killed.
38 In other words, withholding the guerrillas' ability to move, militarily, towards becoming a regular army while exhausting the army they are fighting and finally winning a decision against it. This is the essence of the three-stage doctrine as Mao defined in his 1937 book *On Guerrilla Warfare*. See: Tal Tovy, *Guerrilla and Counter-Guerrilla: Mao's Military Legacy* (Jerusalem: Carmel, 2010), pp. 42-57.
39 Terry Griswold and D. M. Giangreco, *Delta: America's Elite Counterterrorist Force* (Osceola: Zenith Press, 1992), pp. 78-87; Steve Crawford, *The SAS Encyclopedia* (Miami: Lewis International, 1998), pp. 266-69.
40 Ken Connor, *Ghost Force* (London: Cassell, 2001), pp. 303-40.
41 For a description of the incident, see: James Adams and others, *Ambush: The War between the SAS and the IRA* (London: Pan Books, 1988), pp. 110-18.
42 *FM 7-98*, Chapter 7: Combat Support, 7-6: Attack Helicopter Units.

Are Cyber Weapons Effective Military Tools?

Emilio Iasiello

Cyber-attacks are often viewed in academic and military writings as strategic asymmetric weapons, great equalizers with the potential of leveling the battlefield between powerful nations and those less capable. However, there has been little evidence to suggest that cyber-attacks are a genuine military option in a state-on-state conflict. In instances of actual military operations (e.g., Afghanistan, Georgia, Iraq, and Israel/Gaza), there is little accompanying evidence of a military conducting cyber-attacks against either a civilian or military target. Given that some of the nation states that have been involved in military conflict or peacekeeping missions in hostile areas are believed to have some level of offensive cyber capability, this may be indicative. More substantive examples demonstrate that cyber-attacks have been more successful in non-military activities, as they may serve as a clandestine weapon of subterfuge better positioned to incapacitate systems without alerting the victims, veiling the orchestrator's true identity via proxy groups and plausible deniability. Consequently, this paper provides a counter argument to the idea that cyber tools are instrumental military weapons in modern day warfare; cyber weapons are more effective options during times of nation state tension rather than military conflict, and are more serviceable as a signaling tool than one designed to gain military advantage. In situations where state-on-state conflict exists, high value targets that need to be neutralized would most likely be attacked via conventional weapons where battle damage assessment can be easily quantified. This raises the question: are cyber weapons effective military tools?

Key words: cyber-attack, cyber weapons, state-on-state conflict.

Emilio Iasiello has more than 12 years' experience as a strategic cyber intelligence analyst, supporting US government civilian and military intelligence organizations, as well as a private sector company providing cyber intelligence to Fortune 100 clients.

Terminology

There is no international consensus on the definitions for "cyber-attack" and "cyber weapon." However, it can be agreed that these terms refer to the execution of malware with the objective of denying, disrupting, degrading, destroying, or manipulating information systems or the information resident on them. Taking this into consideration, the following definitions have been adopted for this paper:

- **Cyber-Attack**: "actions taken through computer networks designed to deny, degrade, disrupt, or destroy an information system, an information network, or the information resident on them."
- **Cyber Weapon**: this paper accepts the definition created by Thomas Rid and Peter McBurney: "a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."[1]Examples include distributed denial-of-service (DDoS) attacks and the insertion of malware designed to destroy information systems or the information resident on them.

Cyber as an Asymmetric Weapon

Military writings on cyber warfare – a subset of the larger information warfare umbrella – frequently cite critical infrastructures as key targets for military action during times of conflict, as they are seen as enablers of a nation state's military capabilities. The U.S. Department of Homeland Security defines critical infrastructures as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[2] Cyber-attacks in the information environment are important facets of force projection, particularly against soft targets such as communication systems, ports, airports, staging areas, civilian populations, critical infrastructure, and economic centers. In this context, cyber weapons are an ideal embodiment of an asymmetric strategy: the more technically sophisticated a powerful nation's information infrastructure, the more vulnerable it is to cyber-attacks.

Nation State Writings on Information Warfare

The fundamental principle of an asymmetric strategy is to convert the adversary's perceived strength into its weakness. Certainly, in no other area

is this best exemplified than in the cyber domain where the very software and hardware complexities that increase military and societal effectiveness and productivity are also fraught with exploitable vulnerabilities. Academics and military theorists have been contemplating information warfare for many years. In the United States, the earliest reference to information warfare can be attributed to Dr. Tom Rona in the 1970s.[3] The first military adoption of this term was in 1992, when the U.S. Department of Defense published a more formalized definition of information warfare in its classified TS3600.1 policy document.[4] The U.S. military altered the definition throughout the years but the term had become part of its lexicon even if there were no formalized strategies to guide implementation during wartime.

The U.S. was not alone in cultivating progressive thinking on the nature of information warfare and how it could be leveraged for maximum effect. Chinese and Russian military theorists also wrote extensively on the topic. While initial writings seemed more of a mirroring of earlier published material, they did contemplate how such tools could be used as an implement of war. Despite cultural nuances, all agreed on the potential of information warfare as a weapon to bridge the differential gap between superior and inferior forces providing the latter with the means to strike without risking full force-on-force engagement. "Asymmetric" highlights this sentiment, and as one writer described it, is "roughly akin to the Japanese martial art of jujutsu, which is based on the idea that an opponent's strength and energy may be used against him rather than directly opposed with strength of one's own."[5] Unlike nuclear weaponry that requires significant resources and capability for production and management, information war and its instruments are easily accessible to the masses.

Chinese Writing on Information Warfare

The earliest Chinese writing on information warfare is probably the book entitled "Information Warfare," published in 1985 which had later become an article in the Liberation Army Daily.[6] However, it wasn't until Operation Desert Storm that Chinese theorists saw a military using advanced technology to defeat an opponent. In 1995, People's Liberation Army (PLA) Major General Wang PuFeng wrote "The Challenge of Information Warfare" frequently referencing U.S. information warfare efforts against Iraq.[7] Another writer saw this battle as a "great transformation" where information and command and control revolutionized the battlefield.[8]

Scholars considered "information dominance" a key concept to obtaining victory in future wars.

Two Chinese military doctrinal writings, the *Science of Strategy* and the *Science of Campaigns*, acknowledge information warfare as an important military tool for countering a superior adversary's informational and technological advantages. Influential military strategists from prominent Chinese military academies and schools have suggested that China's military should implement cyber or precision-weapon attacks against such critical infrastructure targets as ports and airports. Indeed, many of the more authoritarian writings regarding Chinese military thought advocate this course of action. In the *Science of Campaigns*, the author posits that information warfare is to be used:

> At the critical time and region related to overall campaign operations, to cut off the enemy's ability to obtain, control, and use information, to influence, reduce, and even destroy the enemy's capabilities of observing, decision-making, and commanding and controlling troops, while we maintain our own ability to command and control in order to seize information superiority, and to produce the strategic and campaign superiority, creating conditions for winning the decisive battle.

China's Integrated Network Electronic Warfare (INEW) theory places peacetime and wartime computer network attack and electronic warfare under one authority. Its mission is to disrupt the opponent's ability to process and use information. The strategy is characterized by the combined employment of network tools and electronic warfare weapons against an adversary's information systems in the early phases of a conflict.[9] According to Chinese thought, the strength of such attacks lies in its ability to surprise the enemy to great effect. A controversial text authored by two then- PLA colonels underscores the potential of cyber-attacks against the financial institutions of superior states,[10] particularly as a first strike option. According to James Mulvenon, a noted Chinese information warfare expert, "PLA writings generally hold that information warfare is an unconventional warfare weapon, not a battlefield force multiplier... that will permit China to fight and win an information campaign, precluding the need for military action."[11]

While information war encompasses a broader space of engagement, cyberspace is but one part of the larger information domain. Information

space refers to "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself."[12] Per China's perspective, the main function of the information space is "for people to acquire and process data... a new place to communicate with people and activities, it is the integration of all the world's communications networks, databases, and information, forming a landscape."[13] As such, China sees a larger threat space extending beyond the digital confines of the Internet.

Russian Writing on Information Warfare

Like China, Russia refers to "information space" as a holistic term. In 2010, the Russian government updated its Military Doctrine in which "cyber warfare" was notably omitted (like the Chinese, the Russians use the term "information" rather than the more popularized term "cyber"). However, there were several references to "information warfare" that by definition would include offensive attacks against information systems (i.e., computers) and/or the information resident on them. More importantly, the doctrine recognized the information space as a critical area that the military must protect from outside threats. This bolsters dictums in Russia's 2000 Information Security Doctrine, in which the protection against foreign harmful information and the promotion of patriotic values were identified as national security objectives.[14] Other objectives cited in the 2010 *Military Doctrine* include:[15]

> ...developing goals and resources for information warfare..... to create new models of high-precision weapons and develop information support for them...prior implementation of measures of informational warfare in order to achieve political objectives without the utilization of military forces.

Russian information warfare theory is rooted in the idea that Russia must "respond with war to the information war waged against Russia,"[16]and covers a broad range of actions including political, economic, cultural, and military, to name a few. Russian authors understand information warfare as influencing the consciousness of the masses as part of the rivalry between the different civilian national systems adopted by different countries in the information space. These are put into effect by use of special means to control information sources as "information weapons."[17] Russia defines

"information space" as "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and the information itself."[18] As such, it is the technical (e.g., the physical destruction of an information system a la Stuxnet) and psychological (e.g., influencing and manipulating a population) effect of that space that worries Russia.

Consistent with this broad interpretation of the information space, Russia cites "information weapons" as weapons of concern. By their very definition, information weapons can be used in domains other than cyber, including the human cognitive domain,[19] and include geographic areas where the Russian language is used and a Russian diaspora exists.[20] Certainly Russia viewed the successes of the "Color Revolutions" and the "Arab Spring" as examples of failed information and social control.

U.S. Writing on Information Warfare

The U.S. views cyberspace as the networks and systems that comprise its architecture, rather than the entire information environment akin to the Chinese/Russian definition of information space. The U.S. has published numerous strategic and operational pieces providing insight into how the military should operate in the cyber domain via information operations (IO), of which cyber operations (aka "cyber warfare") is but one of several components. The 2011 Department of Defense's Strategy for Operating in Cyberspace as well as the 2012 revision of its Joint Publication on Information Operations (JP 3-13) reflects recent U.S. military thinking on cyberspace as a warfare arena. Indeed, the establishment of U.S. Cyber Command (CYBERCOM) is in line with the U.S. commitment to operating freely in cyberspace while hindering the adversary's capabilities. According to the Strategy document, CYBERCOM reflects the following goals:

> To ensure the development of integrated capabilities by working closely with Combatant Commands, Services, Agencies, and the acquisition community to rapidly deliver and deploy innovative capabilities where they are needed the most.[21]

The JP 3-13 provides information as to the deployment of cyber capabilities. It sets forth doctrine and guidance governing the activities of the U.S. military in joint operations. According to JP-313:

> Information operations (which include computer network operations) are designed to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.[22]

The key difference between the writings of China/ Russia and the U.S. lies in a holistic interpretation versus a more narrowed perspective of the threat space. China/ Russia prefer to combine the human and technological aspects, while the U.S. focuses solely on the technological aspects. The U.S. views a larger IO campaign as consisting of several separate, albeit possibly interrelated, military capabilities, whereas China/ Russia emphasize a more interconnected perspective where there is no clear separation between the activities conducted or the effects achieved. In this context, a cyber-attack can consist of malware deployment against a critical infrastructure (per the U.S. perception), or hostile information directed against the government or its populace by adversarial oppositionist forces (per the China/Russia perceptions).

Cyber-Attack Incidents

Several high profile cyber-attacks reveal an evolution from disruptive to destructive force. This is not to say that all future cyber-attacks will involve the destruction of information systems, only that in certain instances where opposing factions are entrenched in diplomatic confrontation, precedent has been established where destruction may be a viable option. In the incidents highlighted below, nation state direction or sponsorship was largely suspected but never proven, suggesting that if governments were involved in orchestrating attacks, they preferred to use them as surprise weapons during times of diplomatic tension, with plausible deniability, and in engagements with limited or non-existent force-on-force operations.

2013 South Korea Wiper Malware

In March 2013, "wiper malware" deleted data on three South Korean banks' systems and their insurance affiliates, as well as three broadcasting organizations. While the majority of the attacks occurred on March 20, evidence suggested that in some cases systems have been previously infected with malware set to deploy on that date.[23] The malware overwrote the Master Boot Record of the computers running these networks, as well as disabling

the antivirus program from a well-known South Korean company.[24] The attack was estimated to have compromised 48,000 computers.[25]

This event marked the fourth in a series of well publicized attacks employing wiper malware, the first being the April 2012 wiper malware against Iran's Khang Island facility, the second being the Saudi Aramco incident, and the third being the Qatari RasGas incident. Notably, this indicates a shift toward more destructive attacks by non-state actors during times of political tension. Like the Aramco incident, a previously unknown group ("WHOIS") claimed responsibility,[26] though the reliability of this attribution was called into question due to the questionable history and demonstrated capability to execute this level of attack.

South Korean officials believed North Korea military intelligence units were responsible, operating from Chinese IP addresses.[27] In the frameworks of the prolonged north-south conflict, political and diplomatic rhetoric has often spilled into the cyber domain at least since 2009 when botnets directed DDoS attacks against South Korean and U.S. websites.[28] Prior to March 2013, North Korea ramped up its threats against South Korea and the U.S. during the March 11-21 joint Key Resolve military exercises (which occurred right after the North Korean testing of its nuclear device in February 2013).[29] If North Korea was behind the attacks, they represented a divergence from a usually robust albeit benign DDoS activity. More importantly, the incident signaled to Seoul that the North was capable of conducting destructive cyber-attacks if it perceived transgressions against established "norms" between the two governments.

2012 Saudi Aramco Wiper Malware

In August 2012, a virus erased data on three-quarters of the corporate computers of Saudi Aramco, Saudi Arabia's national oil company, largely considered the world's most valuable company.[30] The malware was designed to accomplish two objectives: 1) replace the data on hard drives with an image of a burning American flag and report a list of infected addresses back to a computer inside the company's network, and 2) wipe the memories of the infected computers.[31] Labeled "Shamoon," the virus destroyed the hard drives on 30,000 computers.[32]

The event's significance lay in the fact that malware was purposefully deployed to destroy as many computer hard drives as possible in a company involved in critical infrastructure. The malware's sophistication is debatable; then-U.S. Defense Secretary Leon Panetta referred to the Shamoon virus

as a very sophisticated tool,[33] while other security researchers from Kaspersky Lab suggested that coding errors in the code were indicative of amateurish work and the malware could have been more destructive.[34] The virus was released against Aramco the day before one of the holiest nights of the Islamic year.[35] This suggests that the attackers wanted to enhance operational success, correctly estimating that there would be limited monitoring during this period, allowing time for the virus to deploy and spread. The attack impacted oil production as well as business practices of the company as some drilling and production data was probably lost.[36] According to one source, it took ten days to replace infected hard drives.[37]

Though a previously unknown activist group called "The Cutting Sword of Justice" claimed responsibility for the attack, stating that it was a response to Saudi policies in the Middle East,[38] many people including unnamed U.S. government officials suspected Iranian involvement.[39] If Tehran was the orchestrator, it preferred to engage Saudi Arabia covertly using a proxy in order to maintain plausible deniability, particularly as the attack directly targeted a major global oil producer and critical infrastructure. While there has been no international consensus as to what constitutes a "red line" in cyberspace, it would stand to reason that the purposeful destruction affecting a global enterprise would be considered an act of force as defined by the International Humanitarian Law of Armed Conflict, which regulates the conduct of armed hostilities between nation states. In this context, the targeting of Saudi Aramco – a symbol of Saudi power – could be interpreted as an Iranian signal to Riyadh of its discontent regarding Aramco benefits from U.N.-imposed sanctions on Iran, as well as Riyadh's perceived collaboration with the U.S. over Iran's nuclear aspirations.

2010 Stuxnet Attack on Iranian Centrifuges

Stuxnet is believed to be closely related to three other equally, if not more sophisticated, malware items known as Duqu, Flame, and Gauss. Since their purposes are more consistent with cyber espionage, they are not included in the current paper.

In 2010, Tehran disclosed that a cyber-weapon, coined "Stuxnet" by a Microsoft researcher, had damaged gas centrifuges in an Iranian uranium enrichment facility. Stuxnet was described as a "highly sophisticated" and complex application designed for the sole purpose of sabotaging uranium enrichment centrifuges controlled by high-frequency converter drivers used by the uranium enrichment facility at Natanz.[40] Approximately 1,000

centrifuges were impacted by the malware, causing them to spin out of control and ultimately require replacement.[41]

Stuxnet was significant in that it was the first incident of a cyber-weapon created and deployed with the intent of degrading, disrupting, and destroying a specific information system. Perhaps more importantly, the malware's sophistication, as well as its clandestine appearance on an industrial control system network air-gapped from the Internet in a secured environment pointed directly at nation state sponsorship. Despite being discovered in 2010, Stuxnet is believed to have been deployed as early as 2009,[42] indicating that a surreptitious delivery against this target was a successful approach. No other group assumed responsibility.

Iran had made it clear on several occasions that it intended to exercise its sovereign right to develop its nuclear program for peaceful purposes,[43] causing great concern for the U.S., as well as other Western and Middle Eastern states, and even Iran-friendly China and Russia.[44] While Stuxnet remains officially unattributed to any government, it is widely suspected to be the result of a U.S./Israel partnership.[45] The successful deployment negated the need for a conventional military strike that risked escalatory retaliation. If the U.S. was behind Stuxnet, the incident could be interpreted as a U.S. signal to Iran that Washington remained committed to not allowing Iran to enrich uranium for weapons purposes, demonstrating that it was able to reach out and gain access to a sensitive and well protected facility with a weapon of destruction.[46]

2008 Georgia DDoS Attacks

In August 2008, Russian forces invaded Georgia as a result of Tbilisi's decision to launch a surprise attack against separatist forces in South Ossetia.[47] Prior to the Russian counter invasion, cyber-attacks were already being launched against Georgian governmental websites.[48] Lasting for most of August, these digital attacks consisted mostly of website defacements (particularly against government websites) and DDoS attacks that targeted media sites, financial institutions, a Georgian hacker community site, and Georgian government sites.[49]

The cyber-attacks were notable for one main reason: they coincided with the Russian military invasion. In many ways, the 2008 cyber-attacks were very similar to the 2007 attacks: defacements and DDoS targeted the private and public sectors. The uniqueness of these attacks lay in their coordination and intensity, as opposed to gradual coordination as was the

case in Estonia.[50] If the same actors or types of actors were involved, they made adjustments to their attack methodology for maximum effectiveness.

Like in Estonia, the attacks were attributed to Russian nationalistic hackers, with Moscow suspected as being their sponsor.[51] If Moscow was again the orchestrator, these attacks could be interpreted as a "lessons learned" exercise in targeting a country via cyber weapons. While infrastructure was the main target in Estonia, media and news organizations were the prime victims in Georgia. By targeting these outlets, the attackers sought to control Georgia's information space and prevent anti-Russian sentiment from being broadcast, a Russian information warfare concept conveyed by leading Russian information warfare theorists such as Igor Panarin.[52] Ultimately, however, these efforts to control information failed, with many believing that Georgia won the information war.[53] Nevertheless, this incident demonstrated that even during force-on-force engagement, Moscow preferred to maintain plausible deniability. One would think that once physical strikes were conducted, the need to conceal cyber operations – particularly if they were not seeking to destroy information systems or the information resident on them – would be moot, especially when considering a nation state that is equal to the U.S. in cyber capability.[54] Nevertheless, the Georgian DDoS attacks signaled to Russia's neighbors and former states that they may be targeted by the same type of activity should their governments enter heightened periods of diplomatic tension with the Russian Federation.

Actual Military Conflict

Not all military-on-military or force-on-force engagements featured cyber-attacks as a primary or supporting military component. This bears noting given that some of the countries involved are capable actors known to have formalized doctrinal writings on how cyber-attacks could and should be used in conflict scenarios. While the absence of strategic cyber-attacks could be interpreted as a lack of viable strategic cyber targets, evidence suggests they were not employed largely because no strategic advantage would be gained, thereby calling into question the efficacy of cyber-attacks as viable weapons to achieve similar results as conventional weapons.

2014 Israel-Hamas Crisis

In July 2014, Israel launched a missile at Gaza's only electricity plant causing the termination of all electricity in the area, which would worsen existing

problems with water and sewage, according to press reports.[55] The use of conventional weapons against this target could have been prompted by Israel's inability to successfully target the plant via cyber means. However, this seems implausible based on Israel's reputation as a leading cyber power and its suspected involvement in some well publicized cyber incidents such as the 2012 cyber-attacks targeting a power plant and other Iranian industries,[56] the 2010 Stuxnet attacks against Iranian nuclear centrifuges,[57] and the 2007 cyber-attacks against Syrian air defense systems.[58] In order to achieve the strategic objective of disabling a key target, it can be inferred that the implementation of kinetic weapons was preferred as a more reliable course of action to support the immediate objectives of the mission.

2014 Ukraine-Russia Crisis

During the 2014 Ukraine-Russia crisis, the Ukrainian telecommunications company Ukrtelecom reported that armed men raided its facilities in Crimea on February 28 and tampered with fiber optic cables, causing outages of local telephone and Internet systems.[59] Given assessments of Russia's proficiency in cyber operations,[60] as well as the fact that much of Ukrainian telecommunications was built when it was part of the Soviet Union, one would think that a cyber-attack would be a feasible course of action given knowledge of the target and the benefits of disrupting cyberspace. Previous Russian nationalist hacker activity (e.g., 2007 Estonia and 2008 Georgia) would further suggest that such an action could have been viable, if not preferential. However, cyber-attacks against the Ukraine did not ensue. Furthermore, while open source reports referenced "cyber skirmishes" transpiring between pro-separatist and pro-Ukraine interests, as of June 2014 there was no evidence of significant activity impacting key critical infrastructure or command-and-control targets.

2013 Syrian Civil War

According to a 2014 *New York Times* article, when Syria experienced an uprising against its government, the Pentagon and the National Security Agency developed a battle plan that featured a sophisticated cyber-attack on the Syrian military and President Bashar al-Assad's command structure.[61] However, according to the same article, President Obama turned it down (as well as other conventional strike options) based on the limited strategic value of the mission, coupled with the untested ability of cyber weapons during a military conflict.[62] The Obama administration remained unsure

whether cyber weapons were a useful military tool, or if they should be reserved for covert operations.[63]

2011 Libyan Civil War

In 2011, the U.S. considered deploying cyber weapons against Libya. According to open source reports, the goal would have been to break through the Libyan government's firewalls to sever military communications links and prevent early-warning radars from gathering information and relaying it to missile batteries aimed at NATO warplanes.[64] However, once the U.S. militarily committed to the use of force, the U.S. relied on conventional weapons to accomplish the same task. While there has been some debate as to the reason behind this (two popular beliefs are that the U.S. did not want to show its capabilities, and it did not want to be the first to use cyber-weapons in this manner),[65] perhaps a more pressing concern was whether or not cyber-attacks could have achieved the same level of military effectiveness as conventional missile strikes.

Conclusion

There is little doubt that foreign governments are developing cyber capabilities, whether to bolster their respective intelligence collection apparatuses or as instruments of nation state power. The military and academic writings of three prominent nation states advocate the use of cyber weapons, particularly against critical infrastructures, in time of state conflict. History is ripe with incidents in which a military targeted an adversary's critical infrastructures during wartime for both tactical and strategic advantage. Therefore, it follows that computer-based weapons could be leveraged in a similar manner.

Nevertheless, most of the observed cyber activities executed against state targets have come during times of diplomatic tension and conducted largely by non-state actors operating as state proxies. Cyber-attacks have been most effective as first-strike weapons benefiting from surprise and the anonymity afforded to them by the difficulties of attribution. In conflicts where military forces were involved (and therefore the need for non-attribution is less important), there were limited instances where cyber-attacks were implemented as either a decisive or supporting component to achieving a military objective. In most cases, physical strikes were the chosen course of action, perhaps as a more reliable and expedient alternative.

In the immediate future, it appears that cyber weapons are better built for surreptitious activity and state signaling rather than as imposing wartime game-changers. That is not to say this will not change in time, but it is going to require nation states to actually use them during conflict, experience the problems that occur during their deployment, and apply lessons-learned to improve their effectiveness. Thus far, this has not been done begging the question: do cyber weapons have a role in conflict? As militaries include technology into their operations, the answer is "yes" – just not a resounding one.

Notes

1 Thomas Rid and Peter McBurney, "Cyber Weapons," *Rusi Journal*, February/March 2012, https://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf.

2 Department of Homeland Security, "What is Critical Infrastructure?" November 1, 2013, http://www.dhs.gov/what-critical-infrastructure.

3 Daniel T. Kuehl, "Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age," *International Law Studies* 76 (2002).

4 "DoD Directive TS3600.1," *IT Law Wiki*, http://itlaw.wikia.com/wiki/DOD_Directive_TS3600.1.

5 Michael Breen and Johsua A. Geltzer, "Asymmetric Strategies as Strategies of the Strong," *Parameters* (Spring 2001), http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2011spring/Breen-Geltzer.pdf.

6 Shen Weiguang, "Focus of Contemporary World Military Revolution—Introduction to Information Warfare," *Jiefangjun Bao* (November 7, 1995): 6.

7 Major General Wang PuFeng, *The Challenge of Information Warfare* (1995), http://fas.org/irp/world/china/docs/iw_mg_wang.htm.

8 Liu Yichang, ed., *Gaojishu Zhanzheng lun* (On High-Tech War) (Beijing: Military Sciences Publishing House, 1993), p. 272.

9 Deepak Sharma, "Integrated Network Electronic Warfare: China's New Concept on Information Warfare," *Journal of Defense Studies* 4, no. 2 (April 2010).

10 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), p. 168.

11 James C. Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, Mulvenon and Yang, eds. (Washington DC: RAND, 1999), pp.175-86.

12 Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian, and English," 2013 5th International Conference on Cyber Conflict, (NATO: CCD COE Publications).

13 Ibid.

14 Doctrine of Information Security of the Russian Federation. (2000). Taken from http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.
15 Russian Military Doctrine (2010). Taken from http://carnegieendowment.org/files/2010russia_military_doctrine.pdf
16 Jolanta Darczewska, "The Anatomy of Russian Information Warfare," *Point of View* 42 (May 2014), http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.
17 Ibid.
18 Giles and Hagestad, "Divided by a Common Language."
19 Ibid.
20 Darczewska, "The Anatomy of Russian Information Warfare."
21 Department of Defense "Department of Defense's Strategy for Operating in Cyberspace – July 2011," http://www.defense.gov/news/d20110714cyber.pdf.
22 Joint Publications 3-13 Information Operations," Department of Defense, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.
23 Matthew J. Schwartz, "North Korea Behind Bank Malware, South Korea Says," *Dark Reading (*April 10, 2013), http://www.darkreading.com/attacks-and-breaches/north-korea-behind-bank-malware-south-korea-says/d/d-id/1109474?.
24 Michael Mimoso, "Theories Abound on Wiper Malware Attack against South Korea," ThreatPost (March 21, 2013), http://threatpost.com/theories-abound-wiper-malware-attack-against-south-korea-032113/77654.
25 Schwartz, "North Korea Behind Bank Malware."
26 "Wiper Malware Analysis Attacking Korean Financial Sector," Dell Secure Works (March 21, 2013), http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector/.
27 Sean Gallagher, "North Korean Military Blamed for Wiper Cyber-Attacks against South Korea," ArsTechnica (April 10, 2013), http://arstechnica.com/security/2013/04/north-korean-military-blamed-for-wiper-cyber-attacks/.
28 Choe Sang-Hun and John Markoff, "Cyber-Attacks Jam Government and Commercial Websites in U.S. and South Korea," *New York Times* (July 8, 2009), http://www.nytimes.com/2009/07/09/technology/09cyber.html.
29 Comprehensive Nuclear Test Ban Treaty Organization, "On the CBTO's Detection in North Korea," February 12, 2013, http://www.ctbto.org/press-centre/press-releases/2013/on-the-ctbtos-detection-in-north-korea/.
30 Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S Sees Iran Firing Back," *New York Times* (October 23, 2012), http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all.
31 Ibid.

32 Kelly Jackson Higgins, "The Long Shadow of Saudi Aramco," *Dark Reading*, October 14, 2013, http://www.darkreading.com/attacks-breaches/the-long-shadow-of-saudi-aramco/d/d-id/1140664?.

33 Phil Stewart, "Shamoon Virus Most Destructive Yet for Private Sector, Panetta Says," *Reuters* (October 11, 2012), http://www.reuters.com/article/2012/10/12/us-usa-cyber-pentagon-shimoon-idUSBRE89B04Y20121012.

34 Fahmida Y. Rashid, "Coding Errors in Shamoon Malware Suggest It May Be the Work of Amateurs," *Security Week*, September 12, 2012, http://www.securityweek.com/coding-errors-shamoon-malware-suggest-it-may-be-work-amateurs.

35 Paul Roberts, "Whoddunnit? Conflicting Accounts on Aramco Hack Underscores Difficulty of Attribution," Naked Security, October 30, 2012, http://nakedsecurity.sophos.com/2012/10/30/whodunnit-aramco-hack/.

36 John Roberts, "Cyber Threats to Energy Security as Experienced by Saudi Arabia," Platts, November 27, 2012, http://blogs.platts.com/2012/11/27/virus_threats/#comments.

37 Roberts, "Whoddunnit?"

38 Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back."

39 Siobhan Gorman and Julian E. Barnes, "Iran Blamed for Cyber Attacks," *Wall Street Journal*, October 12, 2012, http://online.wsj.com/news/articles/SB10000872396390444657804578052931555576700.

40 Matthew Schwartz, "Stuxnet Launched by United States and Israel," *Information Week*, June 1, 2012, http://www.reuters.com/article/2011/12/02/us-cyberattack-iran-idUSTRE7B10AV20111202.

41 Ellen Nakashima, Greg Miller, and Julie Tate, "U.S. Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *Washington Post*, June 19, 2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

42 "Stuxnet Effect: Iran Still Reeling," Industrial Safety and Security Source, August 3, 2011, http://www.isssource.com/stuxnet-affect-iran-still-reeling/.

43 "Timeline of Iran's Controversial Nuclear Program," *CNN*, March 19, 2012, http://www.cnn.com/2012/03/06/world/meast/iran-timeline/.

44 Max Fisher, "Nine Questions about Iran's Nuclear Program You Were Afraid to Ask," *Washington Post*, May 19, 2013, http://www.washingtonpost.com/blogs/worldviews/wp/2013/11/25/9-questions-about-irans-nuclear-program-you-were-too-embarrassed-to-ask/.

45 David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.

46 Emilio Iasiello, "Cyber-Attack: A Dull Tool to Sharpen Foreign Policy," 2013 5th International Conference of Cyber Conflict, 2013, http://www.ccdcoe.org/publications/2013proceedings/d3r1s3_Iasiello.pdf.

47 Council of Europe Parliamentary Assembly Resolution 1633 (2008) on "The Consequences of War Between Georgia and the Russian Federation," available at http://assembly.coe.int/ASP/Doc/XrefViewHTML.asp?FileID=12031&Language=en.

48 EnekenTikk, KadriKaska, and LiisVihul, "International Cyber Incidents: Legal Considerations," Cooperative Cyber Defense Center of Excellence, 2010, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

49 Ibid.

50 Eneken, Kadri and Liis "International Cyber Incidents."

51 Ibid.

52 Darczewska, "The Anatomy of Russian Information Warfare."

53 Clifford J. Levy, "Russia Prevailed on the Ground but not in the Media," *New York Times*, August 21, 2008, http://www.nytimes.com/2008/08/22/world/europe/22moscow.html?_r=0.

54 Keir Giles, "Information Troops – a Russian Cyber Command?" 2011 3rd International Conference on Cyber Conflict (CCD COE Publications: 2011), http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussianCyberCommand-Giles.pdf

55 Alan Greenblatt, "Israeli Bombing Ruins Gaza's only Power Plant," *NPR*, July 29, 2014, http://www.npr.org/blogs/thetwo-way/2014/07/29/336386340/israeli-bombing-destroys-gazas-only-power-plant.

56 Rick Gladstone, "Iran Blames US and Israel for Spree of Cyber Attacks," *Sydney Morning Herald*, December 27, 2012, http://www.smh.com.au/it-pro/security-it/iran-blames-us-and-israel-for-spree-of-cyber-attacks-20121226-2bwa1.html.

57 Ellen Nakashima and John Warrick, "Stuxnet Was Work of US and Israel, Experts Say," *Washington Post*, June 2, 2012, http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

58 John Leyden, "Israel Suspected of Hacking Syrian Air Defenses," *The Register*, October 4, 2007, http://www.theregister.co.uk/2007/10/04/radar_hack_raid/.

59 Polityuk, P. and Finkle, J. "Ukraine Says Communications Hit, MPs Phones Blocked." *Reuters,* April 3, 2014, Taken from http://www.reuters.com/article/2014/03/04/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304.

60 Smith, D., *Russia Cyberoperations* (Washington, D.C.: Potomac Institute Cyber Center, 2010), http://www.potomacinstitute.org/attachments/article/1273/Russian%20Cyber%20Operations.pdf.

61 David E. Sanger, "Syria Stirs New U.S. Debate on Cyberattacks," *New York Times*, February 25, 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html.

62 Ibid.

63 Ibid.

64 Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *New York Times*, October 17, 2011, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

65 Jack Goldsmith, "Quick Thoughts on the USG's Refusal to Use Cyberattacks in Libya," Lawfare Blog, October 18, 2011, http://www.lawfareblog.com/2011/10/quick-thoughts-on-the-aborted-u-s-cyberattacks-on-libya/.

The IDF's PR Tactics for Arab Television Channels

Yonatan Gonen

This essay examines the tactics used by IDF representatives in their interviews with Arab television channels to maintain the legitimacy of the struggle against the Palestinians and justify the use of force in that struggle. The essay, based on research analyzing dozens of interviews held by the *al-Jazeera* and *al-Arabiya* networks with IDF spokespeople, shows that the IDF uses three primary tactics to achieve that goal: denial, avoidance of responsibility, and attempts to downplay the perceived measure of aggression of the event in question. In order to transmit their contents persuasively, those interviewed used several methods of rhetoric, such as posing rhetorical questions to the interviewers and posing direct questions to the enemy. The essay presents and provides examples of the tactics used and discusses their implications.

Key words: propaganda, Arab media, war, Palestinians, IDF spokesperson, rhetoric tactics and contents tactics

Introduction

IDF representatives are often called upon to present Israel's position when it comes to the death of innocent Palestinians and the use of banned weapons in the international and Arab media. In recent years, these media appearances, also called "accountability interviews," have become very common. Television networks such as *al-Jazeera* and *al-Arabiya* are eager to interview IDF representatives in the course of military events, as demonstrated during Operation Cast Lead, Operation Pillar of Defense, and the raid on the Turkish ship SS *Mavi Marmara* in May 2010.

Yonatan Gonen is a doctoral candidate in the Communications Department of the Hebrew University in Jerusalem. He would like to thank Dr. Zohar Kampf, senior lecturer in the Communications Department for his major contribution to this study.

How do the IDF's representatives conduct themselves in interviews dealing with the Israeli-Palestinian conflict? What tactics of rhetoric and content do they use in interviews with the Arab media in order to justify the use of force and maintain the legitimacy of the Israeli struggle? This essay seeks to answer these and similar questions, since to date, there is no in-depth analysis of Israeli interviews to Arab media. The essay is based on research involving the analysis of dozens of interviews granted by IDF representatives to Arab television networks both in Arabic and English, providing information about the interviewees' propaganda and justifications methods, shedding light on the Israeli-Arab conflict and the ways in which the media frames it from a slightly different angle than usual.

First, the essay presents the theoretical literature dealing with the topic under discussion, including findings by major studies on the comportment of interview subjects in accountability interviews and the development of the genre of interviews with the other side to a conflict. Next, the essay breaks down the research method selected for the purpose of analyzing the comportment of the Israeli interviewees. The central part of the essay includes the findings of the research arranged by major themes; this is followed by a discussion of these themes and their resulting conclusions as well as a summary.

Tactics of Contents versus Tactics of Rhetoric: Interviewees' Performance in Accountability Interviews

News channels often hold accountability interviews during crises and conflicts.[1] In such interviews, there is an on-air confrontation with a public figure that is required to respond to an event or action generally attributed to that figure or the institutions with which s/he is identified. While the interviewer seeks to examine the background to the event or action, at times while promoting a predetermined agenda, the interviewee seeks to justify the event or action. In accountability interviews, the public often identifies with the interviewer as if s/he were the public's spokesperson. The interviewer is ostensibly asking his or her questions in the name of certain segments of the public, thereby playing the role sometimes called "the court of public opinion." The interviewee, by contrast, is presented as being alien to the viewing public.[2]

In such interviews, the image of the interview subject is placed at significant risk.[3] Preserving a positive image, then, becomes a key goal of interviewees representing a particular institution, such as an army or

government, and it is therefore important that their statements not be criticized or interrupted by the interviewer. Various scholars, including Benoit,[4] have tried to present models for "image repair" in crises, including a variety of possible manifestations, from denial to apology. In order to grant legitimacy to events in question, the interviewees use what research calls "a defensive style of speech."[5] In other words, there is little use of emotion and only a limited degree of justification of the violence.

Interview subjects must use various tactics of rhetoric to transmit, clearly and persuasively, messages linked to image and legitimacy. Media researchers who analyze tactics of rhetoric have found that interviewees mostly engage in evasive maneuvers to avoid saying things clearly, attack the interviewer over the question asked, and repeat certain expressions while turning the question back on the interviewer.[6]

The Enemy Interview: Small Scale Political Drama

An enemy interview used to be a very rare phenomenon until the establishment of international news networks. The regimes controlling local television channels made any sort of media access to anyone declared an enemy very difficult. The development of new media technologies in the mid-1990s and the expansion of the broadcast range beyond national borders changed the rules of national journalism. The channels began broadcasting around the clock and competing for viewership, and government control was dramatically reduced. To provide viewers with alternate points of view, the news channels provided a platform for the enemy, until such presentations became common practice.[7] Examples are the interview with Iraqi President Saddam Hussein on *CBS* shortly before the U.S. invasion in 2003 and the interview with then-Palestinian Authority Chairman Yasser Arafat on Israel's *Channel 1* during the Second Intifada. As the Arabic-language global television networks grew in importance, a similar phenomenon began to occur in those media as well.

Studies analyzing interviews with the enemy focus on the nature of the interview, the professional conduct of the interviewers, and the dynamics created between these journalists and their interview subjects.[8] Studies show that enemy interviews often include exaggerated antagonism and contrariness. Professional antagonism manifested in challenging questions being posed to the interview subject often turns into direct attacks on the subject and everything s/he represents. The enemy interview, then, turns into a subgenre with its own unique characteristics – a small scale political

drama – and stops being something newsworthy. The enemy interview often develops into fierce, even scandalous debate in a public forum. Local publics and their regimes see such interviews as problematic, even perverse.[9]

One may assume that the main newsworthiness in enemy interviews is the simple fact that they are taking place and providing the opportunity for communicating with the other side. In fact, when there are no diplomatic negotiations, journalists doing interviews play the politicians' part. Speaking with the enemy then has the potential of calming tension between the warring sides. While such interviews may certainly serve to highlight hostile positions on the roots of the conflict, they can sometimes also sketch out a potential resolution to the conflict and serve as a simulation of the possible ways of starting and handling negotiations. Nonetheless, the unusual backdrops in which such interviews are held weaken the interviewing journalist's ability to bridge the gap between the sides. Moreover, the pressure brought to bear on the interviewers results in using a significantly different tone from the one they would assume in normal newscast interviews. In enemy interviews, journalists tend to allow themselves to get dragged into the radical fringes – either hyper-hostility or hyper-respect – giving the interview subject a great deal of power.[10] Generally speaking, enemy interviews tend to become emotional confrontations in which each side tries to emerge victorious rather than to listen to one another.

"Our Israeli Army Correspondent": Israelis in the Arab Broadcast Media

Israel's image in the Arab television networks is highly negative. At times, depiction of Israelis resembles that of Jews by the German press in the 1930s. *Al-Jazeera*, for example, accuses Israel of causing many of the ills of the Arab world, which is one of the reasons it is interested in events in Israel and hosts interviews with Israelis. Although Arab networks had already broadcast interviews with Israelis, *al-Jazeera* was the first Arab network to hold interviews with Israelis of the highest government echelons, such as Shimon Peres and Ehud Barak. Many in the Arab world were surprised by these *al-Jazeera* interviews.[11] Some criticized them fiercely, with certain sources going so far as to accuse the network of being "an extension of the Israeli intelligence service."[12]

The Arab broadcast networks increase their coverage during escalations of the Israeli-Arab conflict and present a clear and consistent anti-Israeli line. The IDF, the Prime Minister's Office and the Foreign Ministry therefore

decided to make certain spokespeople available to them to explain Israel's policy to more than 100 million viewers and readers in the Arab world in fluent Arabic (as well as English). These Arabic-speaking Israelis hold interviews with about a dozen Arab networks, including *al-Jazeera* and al-Arabiya.[13]

One of the Arabic-speaking Israeli spokespeople who makes many appearances on Arab television broadcasts is Avihai Edrey, a representative of the IDF Spokesperson's Unit, who on *al-Jazeera* has earned the ironic moniker of "our Israeli army correspondent."[14] In the seven years between the Second Lebanon War and 2013, Edrey gave close to 2,000 interviews with Arab media, some 1,000 of which took place during the Second Lebanon War and Operation Cast Lead. At least one-quarter were given to *al-Jazeera* and *al-Arabiya*.[15] Avital Leibowitz, also a spokesperson with the IDF Spokesperson's Unit, was interviewed for Arab television networks in English. Edrey and Leibowitz are not invited to do long interviews in the television studios and do not engage in dialogue with the interviewers, but are grilled long-distance for an average of about three and a half minutes.[16]

Research Methodoology

The research on which this essay is based conducted a qualitative analysis of contents of the interviews given by IDF representatives to Arab television networks. For the purpose of the study, interviews with IDF representatives given to three major Arab television networks were selected – *al-Arabiya, al-Jazeera* and *al-Jazeera's* English-language channel – at times of violent outbursts in the course of the Israeli-Palestinian conflict. The overwhelming majority of the interviews analyzed were given during escalation or fighting phases, such as Operation Cast Lead, the Turkish flotilla to the Gaza Strip, the events of the 2011 Naksa Day, and others. The interviews were always held remotely, with a split screen showing the network's studio on one side and the Jerusalem or Tel Aviv studio where the interview subject was seated on the other. The interviews were collected through video interfaces on the Internet, primarily *YouTube*, where the Arab television networks, the Israeli speakers or other entities had uploaded them. Some of the uploading of the clips undoubtedly stems from the particular bias of the uploading source, a factor liable to impact the validity of the study's findings. Nonetheless, the fact that these interviews were uploaded by several different sources with different or even contradictory stances may to some degree offset and balance this problem.

The interviews were transcribed and translated from Arabic into Hebrew, with emphasis given to the media discourse and characteristics of discourse in Arab culture. After the transcription, we identified the major recurrent contents and discourse themes. Two key questions underlying this analysis were: what content and reference methods do the interviewees use to justify Israel's use of force, and what methods of rhetoric do they employ to communicate their message to the enemy public. The answers to both questions are presented according to two major meta-categories: content tactics and rhetoric tactics. The content tactics focus on the contents that serve the speakers to communicate their message, i.e., what the message contains. The rhetoric tactics focus on the speakers' methods or rhetoric and comportment to communicate their messages (repeating the message, using terminology from Arab culture, asking their own questions, and so on), i.e., how the message is conveyed.

The Content Tactics

In many interviews, the interviewees denied that Israel had carried out the actions that the Palestinian enemy or interviewer were attributing to it.[17] Thus, for example, Avihai Edrey, from the IDF Spokesperson's Unit, denied that during Operation Pillar of Defense Israel had sworn to the Palestinians that it would "exterminate them," as in the course of that operation the Israeli Air Force had bombed a school in the Gaza Strip and the IDF attacked the area during a visit to the site by the Egyptian Prime Minister.[18] In some of the interviews, the Israeli speakers expressed their denial by pointing the finger at someone else as responsible for the outcome. At times, they also hinted that the reason for civilian deaths in the Gaza Strip was the decision by the enemy (Hamas) to use civilians as "human shields" or fire rockets from populated areas. So, for example, Avital Leibowitz, the IDF Spokesperson's Unit's English-speaker, emphasized that Hamas stores its military supplies in mosques.[19]

In an interview given by Avihai Edrey to *al-Jazeera* during Operation Cast Lead, it was possible to discern two types of denial: simple denial and a transfer of responsibility to the other side. Thus, for example, when asked by the IDF attacks aid and medical workers in the Gaza Strip, he categorically denied it and hinted that any attack may have been the result of stray Palestinian fire.[20]

In most interviews, the interviewees justified Israel's use of power by saying that the enemy was the one that started the fighting and that

Israel was simply responding to provocations against it. When the Arabic-speaking representative of the IDF Spokesperson's Unit was asked by the interviewer about the circumstances surrounding the deaths of the activists on the Turkish flotilla to the Gaza Strip, he said: "The people onboard [the *SS Mavi Marmara*] were planning to confront our soldiers, attack them barbarically, grab their weapons, and shoot them. They are the ones who bear full responsibility."[21] At times, the Israeli speakers threatened that a future provocation by the enemy would result in a response from Israel: "Attacks will be answered by attacks" and "Calm will be answered by calm." In a similar context, Avihai Edrey, during Operation Pillar of Defense, told *al-Jazeera* that "Hamas has absorbed a very powerful blow because of our operation and will receive further blows if it continues its rocket attacks."[22]

The Israeli interviewees tended not to justify military actions that had gone wrong by insisting that the intention had been good. Nonetheless, in various interviews they hinted that IDF actions serve the enemy's people, i.e., the Palestinians. As part of this assertion they also added in some interviews that the Palestinian people are not Israel's enemy, but rather that "the terrorists" were Israel's enemy.

In many interviews, the Israeli speakers stressed the positive measures taken by the State of Israel, in order to strengthen the spectators' positive feelings about the country and reduce their negative perceptions of the action being debated. In some interviews, the interviewees stressed that Israel first and foremost tries to prevent harm to civilians while using the phrase "surgical strike." In one interview, Avital Leibowitz said, "when Israel attacks terrorist organizations within Gaza, it does not target civilians."[23]

The Israeli speakers also stressed Israel's good features, such as it being a democratic, moral state operating on the basis of international law. In several interviews, they even cited some specific good deeds, such as the disengagement plan from the Gaza Strip in 2005 and the opening of the border crossings to Gaza.[24] The fact that Israel operates on the basis of international law was noted, with emphasis placed on the fact that the same law is not applied by the enemy or enemy states. When Avital Leibowitz was asked if Israel uses white phosphorous in its bombings of Gaza, she answered that "Israel uses ammunition according to international law."[25]

In one interview, Avihai Edrey was asked why Israel did not allow the foreign press to freely cover Operation Cast Lead. He answered that it was precisely thanks to the freedom of the press in Israel that the interviewing network, *al-Jazeera* in this case, could cover the events of the operation.

"The foreign press in Israel can cover the war, this military operation, freely. Your own journalist is at the Israeli border next to Gaza. How does this live broadcast take place every single day if Israel prohibits it from happening?"[26]

Another tactic used to reduce the perceived level of aggression of the fighting was asserting that the military action was not as severe as it was being presented. The interviewees presented Israel as a state that strives to and succeeds in causing as little damage as possible to the lives of the enemy side. Thus, the IDF's Spokesperson's Unit's English-language representative made it clear that Israel attacked hundreds of targets in the Gaza Strip during Operation Pillar of Defense yet the number of dead was relatively small.[27]

In about one-third of the interviews, the Israeli spokespeople explained that no nation in the world would sit idly by were it in Israel's position. In about one-half of the interviews, they justified Israel's actions by claiming it was protecting its citizens. Time after time, the interviewees explained that Israel could not refrain from responding, given the enemy's attacks and its citizen's precarious security. In one of the interviews he granted during Operation Cast Lead, Avihai Edrey wondered: "In only the last few days, hundreds of rockets have fallen around the heads of our children, women, old people and men. Is it conceivable we wouldn't protect our citizens? Is it conceivable that the situation in Gaza continues as usual while the south of Israel is getting hurt?"[28] The speakers sometimes presented the importance of protecting Israel's citizens while noting the difficult conditions in the country's south given the rocket fire from the Gaza Strip. They thus tried to show that not only Gaza Strip residents were suffering because of the fighting. During Operation Pillar of Defense, Avital Leibowitz explained that many Israeli citizens "are, night after night, forced to sleep in bomb shelters" as a result of the rockets fired by Hamas.[29] "We embarked on the operation to defend the citizens of Israel," she said in one interview.[30]

In many interviews, the Israeli speakers attacked whoever was accusing Israel, whether it was a Palestinian or a member of the international corps of journalists, and regardless of whether the accuser was the interviewer. Many times the interviewees accused the enemy of using falsehoods as propaganda and of disseminating lies. For example, after Hamas claimed to have downed an Israeli fighter jet during Operation Pillar of Defense, Avihai Edrey said the following: "Its propaganda terrorism, part of the recurring lies repeated by Hamas, which we've become used to hearing

day and night."[31] Avital Leibowitz, who was asked about supposed "Israeli war crimes" in the Gaza Strip, responded by speaking of "manipulations" by Hamas.[32] The Israeli speakers also explained to their interlocutors, while demonstrating knowledge of power relationships within the Arab world, that Hamas was not getting any support in its battle against Israel, neither from the international community, nor from Arab and Islamic elements and not even from elements within the Palestinian arena itself. Avihai Edrey also noted that the terrorist organizations in the Gaza Strip were endangering countries other than Israel.[33]

The Israeli interviewees sometimes accused the interviewers and their networks of lacking neutrality and presenting inaccurate information. So, for example, in response to an *al-Jazeera* interviewer's claim that Israel was not apologizing for civilian deaths in the Gaza Strip, Edrey attacked her by saying, "Iman, it seems that you're not following the news. Every time there's an error and every time someone who is not involved in hostile activity against Israel is hurt, we at the IDF and I personally at the head, in the name of the IDF, always say in the Arab press that Israel regrets the death of each and every Palestinian civilian not belonging to a terrorist organization."[34]

Edrey's intimate use of the interviewer's given name could be seen as bearing a message of friendship or, alternately, being a way of communicating condescension, part of the "attacker's attack." In that same interview, the interviewer asked Edrey if Israel's strategy involved killing children, whereupon Edrey counterattacked: "It's really funny, Iman, that you should say that the objective of this operation is to kill children. A small number of children have been killed, and we deeply regret it. But the terrorist organizations in the Gaza Strip fire rockets to kill any Israeli."[35] Only rarely did the interviewees apologize for actions attributed to the State of Israel in which children were killed, as Avihai Edrey did this time.

The Interviewees' Rhetoric Tactics[36]

In many interviews, the Israeli interview subject corrected information cited by the interviewers or asked them to prove their assertions. One may think of this type of move as being part of the "attack the attacker" category of rhetorical devices mentioned above. Sometimes the interviewees disagreed with definitions used by the interviewers for a particular term. For example, in an interview dealing with the IDF raid on the *SS Mavi Marmara*, the IDF

Spokesman's Unit representative in Arabic and the *al-Jazeera* interviewer used different definitions for the term "self-defense":

> *Avihai Edrey*: The people onboard [the *SS Mavi Marmara*] were planning to confront our soldiers, attack them barbarically, grab their weapons, and shoot them.
>
> *Interviewer*: What Israel defines as self-defense requires – as leaked by medical reports – the shooting of 30 bullets at a single person? Is that what you call self-defense?
>
> *Avihai Edrey*: First of all, self-defense, in all military words and terms, means that when a soldier feels real danger to his life, he has a right to harm the source of the threat. And that's precisely what happened.

In this case, the interviewer disagreed with Edrey over calling what happened on the ship self-defense, while he defined the meaning of the phrase using the global military lexicon.

In about half of the interviews, the Israeli interview subjects asked the interviewers questions in a kind of role reversal as the interviewee appropriated the role of ceding the floor to the other. The questions the Israeli interviewees posed to the interviewers in these cases assumed two different forms – simple and rhetorical – and at times the interviewees provided the answers to their own questions. In several cases, the interviewees asked the interviewers to pose a similar question to the enemy or directly addressed the enemy, asking them to answer the same or a similar question. Avihai Edrey, for example, asked his interviewer: "In your opinion, why do all the leaders of Hamas hide in mosques or hospitals? Why? Because they know that Israel will not attack these locations."[37]

In some of the interviews, the interviewees expressed their anger that the interviewers denied them the opportunity to complete their statements: "If you only allowed me to finish the sentence, I'd give you the whole story," said Edrey to one interviewer after she cut him off when discussing the targeted assassination of a senior Palestinian activist in the Gaza Strip. The same interviewer continued to cut Edrey off during the interview, until he said: "I would again ask you to give me the right to respond to the questions posed to me. I'm not going anywhere and I'm not going to ignore any question."[38]

An interesting tactic used by interview subjects to corroborate what they were saying was to use contents broadcast by the interviewers' own network. That source would be considered more credible than any other,

making it difficult for the interviewers to attack their subjects. In one of the interviews he gave, Avihai Edrey tried to demonstrate – using contents broadcast by his interviewer's network – that Hamas operatives hide among civilians and use innocent residents as human shields: "Did you see the picture broadcast by *al-Jazeera* a few days ago showing children surrounding a so-called resistance fighter as he was firing an anti-tank missile?"[39] In this example, Edrey tried to suggest that perhaps it was Hamas's fault that medical workers were getting hurt in the Gaza Strip. By saying "so-called," he also sought to make it clear that he was disagreeing with the definition of a Hamas operative as a "resistance fighter." In the same interview, Edrey also used some of the tactics cited above, such as turning the question on the interviewer and pointing an accusatory finger at the enemy.

In some 29 percent of interviews, the Israeli interviewees used expressions, sayings and collocations common in Arab culture. Two expressions were particularly striking: *ahalan wa sahalan* (an effusive greeting that comes from an old saying accentuating Arab hospitality to strangers; "ahalan" means "family," as in "you've come to stay with family," and "sahalan" means a flat land or plain where grass/food is abundant and to be shared with visitors), and an Arabic phrase meaning "he hit me and cried, he got ahead of me and complained." Avihai Edrey used the latter proverb in an interview he gave during Operation Pillar of Defense: "Israel embarked on Operation Pillar of Defense after terrorist factions, headed by Hamas, fired 130 rockets at Israeli areas in the country's south. Therefore, the Israel Defense Force was drawn into [this conflict] and was forced to begin this military operation. Now that the fire and aerial attacks are directed at Hamas [...] some in Hamas have started saying, 'We didn't start the operation. Israel started.' Hamas behaves like the one in the story, 'he hit me and cried, he got ahead of me and complained,' but bears no responsibility for the ramifications of its own acts of terrorism."[40]

The Israeli interview subjects sometimes tried to stress their message via the use of emphatic words. During an interview with *al-Jazeera*, Avihai Edrey said: "We say: we don't want any more escalation."[41] The use of the words "we say" is, in this case, meant to draw the viewers' attention to the next thing the speaker is going to say, i.e., that Israel is not interested in escalation. Avital Leibowitz, the IDF Spokespersons Unit's English-language representative, used a similar technique in an interview she gave during Operation Pillar of Defense: "I only know one thing: we are here to cause serious damage to the terrorist capabilities of as many terrorist

organizations as possible in the Gaza Strip, including Hamas, so that we can live in peace in our homes."[42]

In various interviews, the Israeli speakers repeated the same message several times to demonstrate rhetorical presence and convey their desired message as profoundly as possible. Sometimes the interviewees also reiterated what they had said, using expressions of repetition, as Avihai Edrey did during the Turkish flotilla incident: "As I've already said, and I'll repeat it again: there is a government in Israel. There is a prime minister and there is a decision making echelon that decided to prevent these ships from breaking through the naval embargo on the Gaza Strip."[43]

In some of the interviews, the speakers used visual evidence to support their assertions. The most prominent case was an interview with Avihai Edrey for *al-Jazeera* during which he pulled out a series of photographs proving that Hamas was firing rockets from within densely populated areas. Edrey was asked if, in Israel's opinion, it was permissible to kill civilians in the Gaza Strip, and in responding he, using his pictures, tried to show the interviewer that Hamas was the immoral party to the conflict: "If you want, there are thousands of pictures of mosques, cemeteries, being used to launch rockets [...] If you want, we can dedicate an entire broadcast to show all of the IDF's photos, all of which I gathered from Palestinian sources and news agencies. I'll present [them] to you and we can see who is more moral, the IDF or Hamas."[44]

The overwhelming majority of interviews included the use of first person plural, especially words such as "ours" and "we." Words like that refer not only to the government or the army represented by the speakers, but also to the entire Israeli public in whose name those institutions act. In some of the interviews the interviewees also used the word "you" (plural; Arabic, like Hebrew, distinguishes between the second person singular and the second person plural) when referring to the interviewer's network or the Arab media in general, and "they" when referring to the enemy.

In some 23 percent of the interviews, the interviewees sought to directly address the enemy and/or the enemy people. In an interview given by Avihai Edrey during Operation Cast Lead, he addressed the enemy, saying, "You've just woken up from your illusions. Take the Israeli response and rethink [the question]: what's the future? Do you want bloodshed? Do you want a cycle of war and violence? Why don't you stop these actions, which are useless? Ahalan wa sahalan!"[45]

Alongside the verbal communications, including the meaning of the contents and the semantics of the messages, television appearances also communicate non-verbally in a very profound way. Body language is an inseparable part of the various interviews granted by the Israeli speakers, and in some cases the use of body language helped them communicate their messages. The interviewees' verbal messages, which tried to undermine the enemy's position, were often enhanced by non-verbal messages, such as accusatory and harsh slicing motions with the hands and piercing glares. However, at times, the interviewees' body language communicated messages that were inconsistent with the verbal messages they were trying to get across.

In many interviews, the interviewees gave off an aura of self-control and ease; in some interviews, the interview subjects even smiled. One should note that both IDF speakers, Leibowitz and Edrey, appeared formally in all their interviews, i.e., in uniform, as part of their own military service, and as official IDF representatives. When the interviewees sensed that their answers might arouse some difficulty for them and damage their own and/or Israel's image, they sometimes tried to evade the question, provide ambiguous or partial answers, or change the subject under discussion. A particularly interesting example of such an evasion was an interview given by Avital Leibowitz to *al-Jazeera* in English during Operation Cast Lead.[46] Leibowitz was asked, over and over again, if Israel uses phosphorous; she tried to avoid giving a direct answer at least six times, stressing that the IDF does not give out detailed information about the types of weapons it uses and that Israel acts on the basis of international law.

In order to avoid a situation in which the interviewer and the spectators notice the evasion, the interviewees often tried to give the impression they had no intention of evading questions. So, for example, Avital Leibowitz, made it clear that the IDF does not hide information and that it operates with transparency. Avihai Edrey even used the phrase "I will tell you honestly....," perhaps out of concern that his answer would be seen as an evasion or lie.

Summary and Conclusions

This essay provided a first glimpse at a study of the interviews granted by IDF spokespeople to the Arab media. The essay analyzes their interviews with Arab television networks in order to examine the way in which the interviewees acted to justify Israel's military operations to the Palestinians

and their supporters. The essay presented several tactics of rhetoric and contents used by the interview subjects in order to justify the use of force by Israel in its conflict with the Palestinians.

The Israeli interviews were broadcast mainly during crises when Israel's image is especially at risk. These spokespeople tried to fix that image or at least prevent the negative image from becoming further entrenched. To achieve this end, they used three key content tactics: denial of the actions attributed to Israel and/or casting the blame on the hostile entity; avoiding responsibility while stressing the enemy's provocations and Israel's good facets and actions; and reducing the extent of the event's perceived aggression while stressing the suffering of the Israeli citizens and the enemy's dishonest propaganda.

The interview subjects used several key rhetoric tactics to communicate their forceful messages clearly and convincingly without having to become confrontational. One of the more interesting rhetoric tactics was an attempt at role reversal in which the interviewees turned the questions on the interviewers, thus appropriating the interviewers' role and ceding the floor to the interviewers. They did so even though the interviewee is obligated to answer the questions and is not expected to ask his or her own questions or raise other issues. The questions posed by the Israeli interviewees to their interviewers assumed two forms: simple questions and rhetorical questions.

Another interesting rhetoric tactic used by the interviewees to back up their statements was referring to contents broadcast by the interviewers' own network. The Israeli interviewees demonstrated familiarity with the contents shown by the Arab networks, using the words of the network's journalist or interviewers containing information likely to present Israel in a positive light. Such use of the networks' contents was considered more reliable as the interviewers were hard put denying it on the one hand and using it to attack the interviewees' statements on the other.

A third interesting tactic revealed by the study was the use of phrases, expressions or collocations common in Arab culture, such as ahalan wa sahalan. By using them, the Israeli speaker was trying to address the target audience in its own language and cultural rhetoric. In addition, the Israeli interviewees sometimes tried to stress their messages using phrases of emphasis such as "let's clarify the matter..." or by repeating themselves.

In the overwhelming majority of cases, the Israelis interviewed used the first person plural, especially the words "our" and "we," referring not

only to the government or the army they represent but also the entire Israeli public. In some of the interviews, the interviewees used the word "you" (plural) in referring to the interviewer's network or the Arab media in general, or the word "they" to refer to the enemy. This served to strengthen the dichotomy between the sides, which only perpetuates the hostility between them. In other interviews, the interviewees tried to address the enemy directly, the enemy nation and the television viewers, thus taking advantage of the opportunity to speak to the enemy, as the political world lacks any channel of communication or the opportunity to negotiate.

When the interviewees sensed that their answers were liable to arouse some difficulty or damage their own and/or Israel's image, they often tried to evade the questions, provide partial answers or answers that were open to interpretation, or steer the discussions in a different direction altogether. In a significant number of interviews, the Israeli speakers evaded at least one question posed to them. In order to prevent the interviewers and the audience from noticing the evasions, they often declared they had no intention of evading questions and that they were answering sincerely and honestly. To bring this home, they addressed the interviewers with respect (e.g., "my dear sir") or tried to create an aura of intimacy by moving the conversation to a first-name basis ("Iman").

The Israeli interviewees succeeded in communicating forceful messages to the Palestinian enemy, stress Israel's rock-solid position, deny information, avoid taking responsibility, and try to reduce the perceived level of aggression of the event under discussion, and to do all this without the occasion turning into a bitter confrontation with the interviewers. They almost never expressed regret or an apology for Israel's actions.

The success of the Israeli speakers may be attributed mostly to the tactics of rhetoric they used freely and fluently: posing many confounding questions to the interviewers, using Arabic language expressions, using the contents of the interviewers' own network to back up their assertions, and, on one occasion, pulling out incriminating photographs. These tactics allowed the interviewees to handle the interviews, which in fact resembled interrogations rather than normal television interviews.

One should note that the study on which this essay is based lacks some essential features: one, as noted above, the interviews analyzed were taken from the Internet where they were uploaded by parties that may have their own agendas; representatives of the Israeli establishment, on the one hand, and the broadcasting networks, on the other. The use of this material is

the result of the absence of an Internet interview archive and the refusal of the Arab television networks to provide data, despite repeated requests. Future research will have to analyze more extensive interviews; second, this study focused primarily on the conduct of the interview subject and less so on that of the interviewers (such as types of question, addresses and interruptions) and the deeper dynamic of the interviews; third, the study does not provide an in-depth analysis of the reasons that lead both the Israeli and Arab sides to hold these interviews in the first place. Therefore, future research will have to include in-depth interviews both with the interviewers and the interviewees; four, the findings must be somewhat delimited as it is important to remember that most societies in the Arab world are not democracies and therefore one mustn't expect the interviewer to take a neutral approach in an interview with the Israeli enemy. This needs to be said even though *al-Jazeera* has made its slogan "The opinion and the other opinion"; and last, it is important to remember that this essay refers to the Israeli-Palestinian conflict only and that the only interviews analyzed took place during violent confrontations in the Israeli-Palestinian context alone. Future research should examine the interviewees' tactics during other events, such as the Palestinians' bid for U.N. membership, the Second Lebanon War, and the Arab Spring.

Notes

1 M. Montgomery, "The News Broadcast Interview," in *Communications and Discourse – Studies in Language and Media: A Festschrift in Honor of Shoshana Blum-Kulka*, S. Blum-Kulka, M. Hamo, M. Blondheim and T. Liebes, eds. (Jerusalem: Magnes Press, 2012), pp. 271-302.

2 Ibid.

3 Andreas H. Jucker, *News Interviews: A Pragmalinguistic Analysis* (Amsterdam: John Benjamins Publishing Co., 1986).

4 William L. Benoit, "Image Repair Discourse and Crisis Communication," *Public Relations Review* 23 (1997): 177-86.

5 Gadi Wolfsfeld, Paul Frosh and Maurice T. Awabdy, "Palestinian Television. Covering Death in Conflicts: Coverage of the Second Intifada on Israeli and Palestinian Television," *Journal of Peace Research* 45 (2008): 401-17.

6 John Heritage and David Greatbatch, "On the Institutional Character of Institutional Talk: The Case of News Interviews," in *Talk and Social Structure: Studies in Ethnomethodology and Conversation Analysis*, D. Boden and D. Zimmerman, eds. (Berkley: University of California Press, 1991), pp. 93-137.

7 Tamar Liebes, Zohar Kampf and Shoshana Blum-Kulka, "Saddam on CBS and Arafat on IBA: Addressing the Enemy on Television," *Political Communication* 25 (2008): 311-29.
8 Shoshana Blum-Kulka, Zohar Kampt and Tamar Liebes, "Speaking with the Enemy? Interviews with Palestinians During the Second Intifada," in *30th Anniversary Issue Commemorating the Founding of the Israel Association of Applied Linguistics*, Y. Schlesinger and M. Muchnik, eds. (Jerusalem: Tzivonim Press, 2003), pp. 61-77.
9 Liebes, Kampf and Blum-Kulka, "Saddam on CBS and Arafat on IBA."
10 Ibid.
11 Oren Kessler, "The Two Faces of Al Jazeera," *Middle East Quarterly* (Winter 2012): 47-56.
12 Jeremy M. Sharp, *The Al-Jazeera News Network: Opportunity or Challenge for U.S. Foreign Policy in the Middle East?* (CRS Report for Congress, 2003).
13 Ofir Gendelman, *New Media and National Security*, speech given at a seminar commemorating the late Zeev Schiff, Tel Aviv, the Institute for National Security Studies, 2012, http://www.youtube.com/watch?v=ehXpK2hGGWc.
14 Yoram Binor, interview with Avihai Edrey about Israeli public relations in Arabic, *Channel 2 TV*, October 13, 2007, http://www.youtube.com/watch?v=GBW3vM79udA.
15 Interview with IDF Spokesperson's Unit representative in Arabic, Avihai Edrey, June-July 2013.
16 Kessler, "The Two Faces of Al Jazeera."
17 The transcription in this study uses punctuation as follows: an utterance with a descending intonation is indicated by a dash (-); an utterance with an ascending intonation and having continuation is indicated by a comma and dash (, -); an utterance with an ascending intonation indicating a question is indicated by a question mark (?).
18 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*, November 17, 2012.
19 IDF Spokesperson's Unit interview in English given by Avital Leibowitz to *al-Jazeera* in English, January 11, 2009.
20 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*.
21 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*.
22 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*, November 17, 2012.
23 IDF Spokesperson's Unit interview in English given by Avital Leibowitz to *al-Jazeera* in English, November 14, 2012.
24 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*.
25 IDF Spokesperson's Unit interview in English given by Avital Leibowitz to *al-Jazeera* in English, January 11, 2009.

26 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*, January 6, 2009.
27 IDF Spokesperson's Unit interview in English given by Avital Leibowits to *al-Jazeera* in English, November 17, 2012.
28 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*, December 27, 2008.
29 IDF Spokesperson's Unit interview in English given by Avital Leibowitz to *al-Jazeera* in English, November 17, 2012.
30 IDF Spokesperson's Unit interview in English given by Avital Leibowitz to *al-Jazeera* in English, November 14, 2012.
31 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*, November 17, 2012.
32 IDF Spokesperson's Unit interview in English given by Avital Leibowitz to *al-Jazeera* in English, January 11, 2009.
33 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*, August 8, 2012.
34 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*, February 29, 2008.
35 Ibid.
36 Unlike the content tactics, the rhetoric tactics are not organized on the basis of an existing research model.
37 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*.
38 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*, March 13, 2012.
39 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*.
40 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*, November 17, 2012.
41 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*, March 13, 2012.
42 IDF Spokesperson's Unit interview in English given by Avital Leibowitz to *al-Jazeera* in English, November 14, 2012.
43 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*.
44 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*.
45 IDF Spokesperson's Unit interview in Arabic given by Avihai Edrey to *al-Jazeera*, December 27, 2012.
46 IDF Spokesperson's Unit interview in English given by Avital Leibowitz to *al-Jazeera* English, January 11, 2009.

Non-State Actors: A Theoretical Limitation in a Changing Middle East

Carmit Valensi

The turmoil that has beset the Middle East since December 2010 deepened the instability and surfaced various conflicts and tensions that have been characteristic of the region throughout history. These events reveal the importance of non-state actors in the Middle East and give rise to the need to rethink "facts," terms, and concepts connected to the phenomenon of the nation-state, practically and theoretically. Although non-state actors are not new in the global or Middle Eastern political landscape, it is evident that the theoretical and practical discussion, with its political, military, legal, and international aspects, has remained largely "state" in a way that allows little room for a thorough understanding of non-state phenomena. The purpose of this article is to discuss developments in the Middle East, with an emphasis on the actions of non-state actors as significant shapers of regional processes, while discussing the validity of theories and conceptualizations in international relations for an analysis of existing non-state phenomena. The discussion will involve an analysis of two test cases: Hizbollah and the Islamic State.

Key words: Regional upheaval, non-state actors, terrorist organizations, Hizbollah, ISIS, international relations, constructivism

One of the explanations given for the wave of protests that swept the Middle East four years ago was that the turmoil was a long-term effect of the era of colonialism. Most nation-states in the modern Middle East are relatively new creations, the result of Anglo-French imperialism, which divided the remnants of the Ottoman Empire into states with artificial borders in the Sykes-Picot Agreement. The arbitrary division of states completely ignored

Carmit Valensi is a Neubauer research associate at INSS and a doctoral student at the Tel Aviv University.

the fragile ethnic, religious, and communal fabric characteristic of the region, and the current upheavals are a late outbreak of internal distress arising from that same historical injustice.

Recent developments in the Middle East indicate two main trends: one is the undermining of divisions between states and formal territorial borders, while the other is the growing dominance of non-state actors as shapers of processes.

In regard to the first trend, Iraq has been split into three de facto entities, Sunni, Shiite, and Kurdish, with the Kurds marching toward establishing an independent state. Libya has not succeeded in stabilizing itself since Gaddafi's ouster and is controlled by clans and gangs. Post-Assad Syria could follow suit and crumble to its foundations. South Sudan "celebrated" three years of independence, in the course of which it experienced a violent and bloody civil war, and it was recently ranked first on the index of the world's fragile states.[1]

Not only is the state framework being weakened; primordial sub-state identities—of ethnic group, tribe, or family—and supra-state identities translated into ideas of the Islamic *ummah*, the caliphate, and sometimes even pan-Arabism, are becoming increasingly prominent. Thus, political struggles are painted as Sunni and Shiite struggles, state borders are becoming more fluid, and nation-state identity does not necessarily dictate the tone.

The second trend, which involves the dominance of non-state actors in the Middle East, is not new, but what is new is their scope and intensity. Violent non-state organizations have played a significant role in the region in recent decades: Hamas is in de facto control of the Gaza Strip and continues to walk the line between terrorism and the political and social realms. Hizbollah has been continuously challenging Lebanese sovereignty for the past three decades and is leading the fighting alongside the Assad regime in the civil war in Syria. New jihadi organizations, some of which are official branches of al-Qaeda and others independent, have joined the violent landscape in the region. Recently, the Islamic State (ISIS), which in its previous incarnation was al-Qaeda in Iraq, announced the establishment of the caliphate in areas of western Iraq and eastern Syria and called on other factions in the world to swear allegiance to it. In Syria, the al-Nusra front, a branch of al-Qaeda, declared the founding of an Islamic emirate in the country. The troubling implications for the Middle East of the actions

of thousands of volunteers who are flocking to Syria from around the Arab world and the West remain unclear.

No matter how widespread it is becoming, the phenomenon of non-state actors does not mean the end of the nation-state, which is expected to remain in regional order in the future as well and certainly in states with a stable national basis, such as Egypt and Tunisia. Nevertheless, it is important to recognize that the familiar nation-states are no longer the sole model organizing international relations, either in the Middle East or the rest of the world.

A significant portion of the research literature in political science and international relations on non-state organizations, both in the Middle East and outside the region, suffers from generalizations and uses terms that do not provide an up-to-date solution for analyzing them. In fact, the main approaches continue to give dominant weight to state actors and state practices. Likewise, the theories create a sharp and rather binary distinction between non-state actors and state actors and ignore many cases in which the boundaries between them are blurred. In contrast, later research approaches allow a more complex understanding of the non-state world.

The main theories in international relations over the years have analyzed the actors influencing the political system, their motives, and the relationships between them and other actors in the system. This article will present the main points of the major approaches in this field; realism, liberalism, and constructivism,[2] and will examine their suitability for describing phenomena in the Middle East. But first, let us define non-state actors.

Non-State Actors

One definition of non-state actors in the literature includes organizations "largely or entirely autonomous from central government funding and control; emanating from civil society, or from the market economy, or from political impulses beyond state control and direction." These organizations act "in ways which affect political outcomes, either within one or more states or within international institutions, either purposefully or semi-purposefully, either as their primary objective or as one aspect of their activities." [3]

It is customary to distinguish among four types of non-state actors.[4] Multinational corporations (MNCs) operate in at least two countries and manage production or deliver services. Generally, they are private companies with headquarters in one country and subsidiaries in others. Non-

governmental organizations (NGOs) are voluntary, not for profit, private, and self-governing. What they have in common is their independence from the government, from large corporations, and from other outside influences. Super-empowered individuals have political, economic, intellectual, or cultural influence. They include industrialists, financiers, media figures, celebrities, religious leaders, and terrorists. Intergovernmental organizations (IGOs) are actors with an official connection to states and are defined as intergovernmental organizations established at the initiative of two or more states that conduct political interaction (the UN).

Along with the ongoing discussion of non-state actors and the focus on their positive contribution to political activity, there has also been extensive discussion of violent non-state actors over the years, and this has gained momentum since September 11, 2001. These actors are defined as organizations that use illegal violence, that is, make use of force that is not acceptable to the state in order to achieve their goals and thus challenge the state's monopoly over violence.[5] The research literature tends to distinguish among terrorist organizations, criminal organizations, quasi-military organizations, militias, freedom fighters, pirates, and guerillas.[6]

The Realist Approach: The State as a Major Actor in International Relations

Beginning in the nineteenth century, nation-states were the most significant units operating in the international system. The realist paradigm has reflected the "state-centric" idea since World War II. Realism developed as a critique of the theory of idealism, which was common in the interwar period and whose aim was to avoid another world war. Hans Morgenthau, in his 1948 book *Politics among Nations*, challenged the assumptions of liberal, idealistic scholars who stressed the importance of public opinion, in the 1920s and 1930s, in shaping foreign policy.

Morgenthau and others argued that classical realism rests on three basic assumptions: 1. the state-centric approach, which assumes that states are the most significant actors in world politics; 2. the principle of rationality, which is that states are considered to be homogeneous and rational actors; and 3. the assumption of power, which is that states seek first and foremost to increase their power, especially militarily, both as a means and as an end. Every policy seeks to maintain, increase, and apply power, and since only states have the resources to enable them to maximize their power, they are the most significant actors in the system. [7]

According to the realists, global political actors are defined by means of three categories: sovereignty, state recognition, and control over a territory and a population. Other entities in the international system cannot be autonomous and distinct because they do not incorporate these three elements.[8] At the height of realism, other non-state actors, whether they were multinational corporations, transnational groups, or terrorist organizations, were perceived as lacking in importance in the international system.[9]

In the 1960s and 1970s, political scientists, including international relations scholars, began to discuss non-state actors as influencers of foreign policy.[10] The focus on these actors stemmed from an ongoing interest in special groups and political and social movements that developed in the 1970s and dealt with subjects such as abortion, gun control, the environment, racism, and human rights. At that time, there were also violent non-state actors such as the National Liberation Front (FLN) in Algeria, the Basque separatist group ETA in Spain, the Baader Meinhof gang (Red Army Faction) in Germany, the Irish Republican Army (IRA), the Kurdistan Workers' Party (PKK) in Turkey, and the Tamil Tigers in Sri Lanka (LTTE).

The prevalence of violent groups in the post-World War II period, which was connected, among other things, to the technological revolution, to processes of globalization, and to changes in transportation,[11] led to an understanding that realism was not able to account for all the structural changes taking place in the international system.

The Liberal-Pluralist Approach

In the mid-1970s, scholars known as "liberal pluralists" arrived at the conclusion that states are not isolated actors in the political system, that they are not necessarily homogenous because they are composed of competing bureaucracies, and that the traditional supremacy of military and security issues as drivers of policy had changed and economic and social interests had become even more important. It was thus increasingly difficult to identify clear boundaries between the fields.[12] The major argument was that international organizations have real or potential power to act and mitigate some of the problems arising from the anarchy characteristic of international relations.

Robert Keohane and Joseph Nye were among the first scholars to call for a reexamination of the state-centric paradigm because it had failed to identify the importance of non-state actors. In a collection of articles

from 1971, they identified interactions that are not state interactions and defined them as "the movement of tangible or intangible items across state boundaries when at least one actor is not an agent of a government." [13]

Another major study from the 1970s, the Non-State Actor Project (NOSTAC), dealt with the importance of non-governmental actors. [14]The researchers looked at events that had taken place between 1948 and 1972 in three regions, Western Europe, the Middle East, and Latin America, in order to empirically explain the growth and behavior of non-state actors. Their findings proved that only one-half of the interactions in these regions had taken place between states, and their conclusions led them to determine that only one-half of international events could be analyzed using the state-centric approach.

Neo-realism and Actors in International Politics

Despite the claim that the realist approach misses events because of its focus on states, a series of events that took place in the late 1970s and early 1980s proved to the researchers that the basic assumptions of realism were still relevant to an analysis of global politics: the tension between East and West and the U.S. arms buildup against the Soviet buildup; the military involvement by the superpowers in Africa, Central America, and southwest Asia; the Yom Kippur War and the Iran-Iraq War. International institutions were unable to shape regional interests and appeared to be extensions of the inter-state tension in the world. These events and the need to explain U.S. hegemony (from an economic perspective as well) led to the development of neo-realism.[15] One of the most prominent neo-realist scholars, Kenneth Waltz, implemented systemic approaches in the realist paradigm that explain the behavior of actors in light of the existing structural constraints in the international system.[16] Waltz argued that the international structure must be defined only by means of the significant actors operating in it and not by all of the actors. In response to accelerated activity by non-state actors and the resulting criticism of realism in the 1970s, Waltz emphasized the role of these actors and argued that while the nature of power had changed (and was divided at that time among different types of actors), its use had not.[17]

Constructivism

In contrast to realism and liberalism, constructivism is not a distinctive political science approach, and its status is that of a broad social theory

and less of a paradigm. This approach gives a central place to ideas in the structuring of social life and thus undermines the approaches that explain social life by means of materialist arguments such as biology, geography, and technology. While these have a role, it is mediated by ideas, which give it meaning. Similarly, the interests and identities of the actors operating in the international system are shaped by their concept of the world, which is socially structured. [18]Alexander Wendt, who is identified with this approach, adopts three main terms: identities, which determine the actors' identity; norms, defined as shared expectations concerning the proper behavior for the actor's identity; and interests, referring to what the actors want to achieve. [19]

The Relevance of the Approaches to an Analysis of Non-State Phenomena in the Middle East: A Critical View

The theoretical analysis enables us to draw a number of conclusions regarding the validity of the main approaches in international relations for describing the current situation in the Middle East.

The realist and neo-realist approaches are still state-oriented and provide relatively little meaning for non-state actors. Criticism of this has grown because of the increase in non-state terror in general and the events of September 11 in particular. The critics' main argument was that this approach cannot explain the consequences of the terrorist attacks for global politics and for the choices of the state actors. In the meantime, a question has arisen as to how the realist approach can explain a situation in which the only superpower in the world declares war on an abstract entity such as terrorism.[20] In general, this approach has had a difficult time explaining actors that are not identified as states and that have an influence, once on the domestic politics of the state in which they operate and a second time on the foreign relations of other states in the region.

Proponents of the neo-liberal approach[21] recognize the importance of non-state actors, but they tend to interpret their interests in economic terms, with little or no reference to the military and security considerations that are at the heart of the neo-liberal approach. In this way, they too miss the ability to discuss non-state organizations that are operating today in the international system and in the Middle East that are not necessarily driven by an economic or social interest. The liberals, like the realists, attribute an external motive for actors, whether anchored in the structure of the political system or in other structures. In fact, the two approaches

assume a linear development of phenomena, that is, that states will remain states (the dissolution of frameworks is not addressed) and violent non-state organizations will have set practices, such as the use of violence for reasons of power or survival. So too, they assume that there is a certain kernel of continuity in the actor's approaches and its ways of coping with its environment. The strength of these approaches is in explaining permanent and ongoing phenomena, but they encounter an obstacle in attempting to explain change and dynamism in the system.

The Middle East, especially in the past four years, is an example of an arena in which state frameworks, organizations, political structures, alliances, and political leaders are fragile and fluid. The actors operating in this arena are characterized by regular, linear, unidimensional patterns of activity, as the realists and liberals tend to assume. Despite the limitations of the comparison between the approaches and constructivism (they are political paradigms and present different parameters for analysis from those in constructivism), it appears that the constructivist approach allows a more accurate look at the phenomenon of non-state actors in the region and their growing influence. The approach recognizes their importance as influential actors and assumes that the nature of the actors is not fixed, but changes in accordance with the context and over time. An emphasis on ideas and norms as a central element in understanding the motivations of the actors (more than the pursuit of power and material benefit), as the approach proposes, is essential for understanding the politics, certainly that found in the Middle East. This argument is twice as valid when discussing violent non-state actors such as terrorist organizations.

Hizbollah and the Islamic State

Hizbollah and ISIS represent two models of non-state actors in the Middle East. Hizbollah challenges the dichotomy between a state and a non-state and constitutes an intermediate phenomenon which blurs the boundary between state actors and non-state actors and also illustrates non-linear organizational practices as a result of its multiple identities. The organization accepts the national order and operates within the Lebanese state framework. ISIS is a later development that undermines the state framework in the Middle East, illustrating a dynamic of dissolution of frameworks and the creation of new spaces that go beyond the known borders of the nation-state. In this sense, it can be argued that ISIS is a supra-national and "a-national" organization.

Hizbollah

The main approaches in international relations place clear boundaries between a state actor and a non-state actor. The case of Hizbollah, like other violent organizations operating in the international system, challenges the unequivocal separation between the two types of actors. Hizbollah is not formally defined as a state and is not recognized as such. It operates within a sovereign state and is defined as a violent non-state actor, as a terrorist and guerilla organization, as an armed political organization, or as an insurgent. However, an attempt to apply the classic definitions of state to the case of Hizbollah shows that it might be thought of as a state.

According to Max Weber's classic definition, "a compulsory political association with continuous organization (*politischer Anstaltsbetrieb*) will be called a 'state' if and in so far as its administrative staff successfully upholds a claim to the monopoly of the legitimate use of physical force in the enforcement of its order."[22] While Weber gives a functional definition, British sociologist Michael Mann proposes an institutional definition, stating that the state contains four main elements, being: (1) a differentiated set of institutions and personnel, embodying (2) centrality, in the sense that political relations radiate outwards from a centre to cover a (3) territorially demarcated area, over which it exercises (4) a monopoly of authoritative binding rule-making, backed up by a monopoly of the means of physical violence.[23]

An analysis of Hizbollah in the spirit of Weber's and Mann's definitions of state reveals that there is significant overlap between the organization's characteristics and those of the state. Thus, Hizbollah operates in a "territorially demarcated area" in the state of Lebanon. It "exercises a certain, even high level of authoritativeness" through effective internal enforcement mechanisms and means of control. Since 1992, it has been a political actor in Lebanese state politics that promotes laws and norms of behavior by means of "legislative processes backed up by political force," and since 2005, it has even been represented by ministers in the government. It operates a network of institutions and infrastructures (social and military) for the residents of Lebanon, including schools, summer camps, hospitals, and charitable organizations, in certain areas on a larger scale than the network run by the state itself. The extent of the organization's legitimacy among parts of the Lebanese population is even greater than that of the state. Hizbollah has representatives in various countries around the world and maintains external relations with Arab states.[24] Nevertheless, it is not a real

state and does not have international recognition. Thus, the organization challenges the conventional conceptions and distinctions.

The use of the word "identities" is likely to assist in understanding the complexity of the organization. Hizbollah is an example of an entity between a state actor and a non-state actor, with a large number of identities that shape its behavior. These many identities create a model different from that of a classic terrorist organization, which primarily has a military identity. Hizbollah has four main identities: it has a state identity, which includes activity in the state political system, a monopoly on the means of force, maintenance of order, provision of welfare and educational services, construction of civilian infrastructures, and the use of significant military force. At the same time, it has a non-state identity, which is reflected in the use of terror and violence, despite the lack of an official monopoly on the means of force, a high level of mobility, and a limited level of institutionalism, with minimal, if any, subordination to laws and international treaties. In its sub-state framework, Hizbollah was founded as a Shiite organization that represents the Shiite population in Lebanon. This identity generally takes precedence over the state identity, and in cases in which it is dominant, it could threaten legitimacy and loyalty to the state. Hizbollah also has a supra-state identity, which embodies a long-term vision to establish a broad, Shiite-dominated Islamic entity. Today this vision is being blurred, more than in the past. It primarily includes Hizbollah's ties with Islamic states and organizations that share its ideology and agenda, particularly Iran and Syria.

A quick chronological look at Hizbollah shows how the movement's different identities have developed over time, been maintained side-by-side, and shaped its patterns of behavior over the years.[25] Hizbollah had a non-state identity between its establishment in 1985 and 1992, the year it decided to take part in the Lebanese political system. During this period, the organization worked in a defined geographic area, and its hierarchical and secret organizational structure reflected the structure of a non-state actor and included limited military capabilities. While maintaining its sub-state identity, which is connected to the Lebanese Shiite community's social and political awakening, Hizbollah, with generous aid from Iran, began to build an educational, cultural, and health system as a solution to the societal, economic, and political distress of the Shiites.[26] Its supra-state identity was greatly influenced by the Shiite revolution in Iran in 1979. The idea, as expressed in many statements by the organization's leaders, was

to establish in Lebanon a state based on Sharia (Islamic law) which would be an integral part of a worldwide Islamic state.[27]

During the 1990s, Hizbollah began to develop a state identity from 1992, when it became a political player, until the IDF withdrawal from Lebanon in 2000. During this process, it expanded from an ideological movement to an established organization characterized by a ramified organizational structure, a significant geographic presence in Lebanon, and an extensive welfare infrastructure. It began to provide for the essential needs of the population, which the state was powerless to fulfill. The movement relied on broad legitimacy and became an active player in the Lebanese political system. At the same time, it retained its previous identities (sub-state and supra-state), although in a more muted fashion, given its ambition to position itself as a Lebanese national organization. In the turn of the 21st century, Hizbollah played the role of an actor that skillfully combined characteristics of a non-state terrorist organization with those of an active political player in the Lebanese political system. Its military achievements (as perceived from its narrative of victory in the Second Lebanon War) positioned the movement as a significant player in the country and expanded its circles of support.

The following decade, in contrast, showed the tension created by Hizbollah's multiple identities and commitments, which to a large extent were contradictory. After a period of military achievements and political consolidation, the movement found itself clearly dedicated to the civil war in Syria, and its position was open to ongoing criticism at home, mainly due to the fear of causing a deterioration in the already fragile situation in Lebanon. Theoretically, it would appear that Hizbollah has invested most of its inputs in the non-state identity and acted like a military organization lacking constraints and responsibility. It has also focused on fulfilling the obligations embodied in its supra-state identity as part of an Islamic resistance alliance consisting of Iran and Syria, largely at the expense of its national image.

Many studies have dealt with the linear transition from violent organization to political player on the basis of the assumption that the political institutionalization of the group, which has operated in an extra-institutional framework until now, would lead to restraint and to adoption of non-violent and accepted rules of the game.[28] However, in recent years, research has actually focused on the combination of violent activity and political participation by the actors. The case of Hizbollah is an example

of an actor that does not make a linear transition from the military to the political while neglecting the first commitment, but that is integrated into a cyclical dynamic, which highlights different spheres of activity in different time periods.[29]

The historic process undergone by Hizbollah and an analysis of its current situation illustrate the importance of recognizing its multiple identities as well as its ability to give varying intensity to its different identities according to the circumstances and needs, as part of the patterns of thought and pragmatic behavior characteristic of the organization. Over the years, in periods of tension between Hizbollah and the Lebanese state, the movement temporarily downplayed the identities that competed with the Lebanese national identity until relations were stabilized, and afterwards, worked to restore its equilibrium until the next challenge. Nevertheless, the current sequence of events in which Hizbollah is involved is a clear example of a clash between identities. One identity—in this case, the supra-state identity and the connection to Iran and Syria—clashes with the Lebanese state identity that the organization has aspired to establish in recent years. This development could undermine the equilibrium and balance between the commitments to various identities, which Hizbollah has attempted to maintain over the years.

An in-depth analysis of organizations such as Hizbollah requires an understanding and recognition of the phenomenon of multiple identities as a factor mediating between the ideological vision and the daily practice. Thus, a dynamic strategy is formed that adapts itself to the circumstances and the context and allows the movement to emphasize identity as dependent on the target audience it is facing at any given moment (the Lebanese government, Israel, or Iran, for example). An analysis that does not taken into account the ideological dimension, the multiple identities (primarily state and non-state), and the behavior derived from them and that focuses on rational cost-benefit considerations could miss the complexity of Hizbollah and its ilk.

The Islamic State

The growth of the Islamic State in the era of regional turmoil is connected to three developments: the rise of radical Islamic ideas as an alternative to the secular order presented by the dictatorships; exploitation of the chaos and entrenchment in areas with limited governance (especially in Syria and Iraq) as a result of the revolutionary winds that swept the region

at the start of the events; and finally, the potential to change the formal territorial borders in the Middle East and undermine the state structure as the exclusive structure in the region.

ISIS was established by Abu Musab al-Zarqawi in 2003, initially called Jama'at al-Tawhid wal-Jihad. Its goal was to fight the coalition forces that had invaded Iraq in order to overthrow the government of Saddam Hussein. About a year later, members of the group pledged allegiance to the central al-Qaeda organization in Afghanistan and became known as al-Qaeda in Iraq. In February 2014, as a result of differences of opinion between al-Qaeda's central leadership and the group's commanders, the leadership decided to distance itself from the group, which, under Abu Bakr al-Baghdadi's leadership, became an independent organization called the Islamic State of Iraq and Syria (ISIS). In late June 2014, when it took control over areas in western Iraq and northeastern Syria, it declared the establishment of an independent Islamic Caliphate in the territories under its control, appointed al-Baghdadi as Caliph, and changed its name to the Islamic State. This change indicates the group's ambitions to cross the accepted boundaries.[30] In order to understand the source of the decision to declare an Islamic caliphate and its potential implications for breaking state frameworks in the Middle East, it is necessary to understand the ideological and religious dimension that is the basis of Islam in general and the organization's ideology in particular.

Like other radical Salafist movements, IS takes its ideological inspiration from the Muslim Brotherhood, which originated in Egypt in the late 1920s. The movement had a fundamentalist interpretation of Islam and called for adopting the way of life of the early fathers of Islam.

Islam is based on the assumption that the community (*ummah*) transcends the state, which is perceived as an artificial product that undermines the natural unity of believers. It is also based on a transnational interaction that enables connections between different Muslim communities in different geographic areas, a space called the House of Islam (*dar al-Islam*).[31] Islam is not only a religious framework, but also a source of social, legal, and economic rules of behavior whose purpose is to regulate relations between Muslims and between Muslims and non-Muslims. Therefore, religion and politics are together embodied in the *ummah* and are not separate, as in the West. The Islamic idea is fundamentally supra-national and supra-state.

The main thinkers who critiqued the state structure and served as a source of inspiration for the Islamic jihadi movements were Sayyid Qutb,

an Egyptian educator and Muslim Brotherhood theorist, and a Pakistani philosopher, Abul A'la Maududi. Both discussed the corruption of the Middle Eastern regimes and the decline of the Muslim world, which they attributed to the abandonment of the straight path of Islam. The solution, they believed, was to revive Islam and apply sharia. They called on Muslims to unite across national borders in order to contend with the power of the West and the negative influences of its culture. Maududi referred to Islam as transcending ethnic and national identity, which is embodied in the state structure.

Those who accept the principles of Islam are not divided by any distinction of nationality or race or class or country. The ultimate goal of Islam is a world-state in which the chains of racial and national prejudices would be dismantled and all mankind incorporated in a cultural and political system, with equal rights and equal opportunities . . . His ultimate goal would be a nation-state rather than a world-state, nevertheless if he upholds any world ideology, that ideology would necessarily take the form of imperialism or world domination, because members of other nationalities cannot participate in his state as equals, they may do so only as "slaves" or subjects.[32]

In a video published on July 28, 2013, ISIS described its doctrine, which is based on two central pillars: The first is eradication of all heretic phenomena in society. This will start with opposition to ideas such as nationalism and communism and habits such as alcohol consumption and prostitution. The Alawites and the Shiites are considered infidels, and so fighting in existing Muslim states (especially Iraq) is more important than fighting the Christians. The second is that the basis of life is Islam. The judicial process in the country will use Islamic law in Islamic courts, and in general, it is important to disseminate knowledge of Islamic law to the ummah. The way to implement this ideology is through jihad.[33]

Beyond the fact that it is a violent non-state actor that subverts state sovereignty, ISIS is different from other terrorist organizations in the Middle East. It presents a unique model that combines a number of elements of the various organizations in the region:

Conquering territory and attempting to establish a state. Most terror and guerilla organizations (such as Hizbollah, Palestinian Islamic Jihad, and al-Qaeda affiliates) do not aspire to conquer territory but use "hit and run" operations to wear down and intimidate the enemy so that it will withdraw from a

territory. IS, in contrast, seeks to conquer territory and take charge of it and to create a governance mechanism.

Although the organization is called the Islamic State, the word "state" may be misleading. It is not used in the modern sense of a nation-state with territorial boundaries, but in an earlier sense that reflects the idea of the Caliphate and an Islamic space not delineated by defined geographical boundaries.

If ISIS does in fact succeed in fulfilling its aspirations, the resulting territorial contiguity could create a new space of its kind in the Middle East that is not derived from the historic Sykes-Picot Agreement and is not subject to law or to international law, but to the Islamic vision.

Managing a civil government and dawah activities. At the early stages of its operations in Syria and Iraq, it was evident that the organization had learned lessons from its conduct toward the civilian population in its previous incarnation as an al-Qaeda affiliate in Iraq. While it started as an organization that slaughtered civilians indiscriminately and concentrated all of its resources on the military struggle, ISIS, especially in light of its economic assets, began to create civil governance mechanisms, to establish a local governmental and legal system, and even to supply the population with basic needs, including food, drink, and fuels at reduced prices.

The publication of *wathika al-madinah* (document of the city) after the recent takeover of Mosul about a month ago lays the foundation for managing civilian life with the appointment of a person responsible for legislation, economics, and trade in the city. It also illustrates the process of entrenchment and management by the organization.[34] ISIS established *shura* councils (governmental consultation groups) and sharia committees whose purpose is to apply religious law. The governors of the region and tribal heads must give *biyah*, an oath of allegiance to the leader, and they are responsible for the existence of the administrative system stretching de facto from Raqqah in Syria to Mosul in Iraq.[35]

Thus, so far, the Islamic State's entrenchment is reminiscent of the development of Hamas and Hizbollah, which combine characteristics of an armed terrorist organization and a political and governmental actor. However, ISIS, unlike Hamas and Hizbollah, does not accept the existing order, and the administrative and political system that it operates is not subject to an existing state framework. ISIS is a fascinating case study of an organization based on a fundamentalist ideology that challenges the

idea of the modern nation-state. A theoretical attempt to analyze it from a dichotomous perspective that places the state opposite the non-state actor could impair understanding of the organization. So too, the ideology that is driving ISIS and its perception of the West and the regimes and infidel populations of the Middle East, must be taken into account when explaining its behavior.

Summary and Recommendations

In a certain sense, the turmoil in the region and the fragile fabric of the Middle East have caused the dissolution of familiar frameworks. The developments described in this article raise anew questions about boundaries, identities, and concepts that have characterized the geopolitical structure of the Middle East until now.

Hizbollah and IS are examples of the range of violent non-state actors with influence over the regional order. Hizbollah is defined as a non-state actor. However, it recognizes the existing order and has practices and behavioral characteristics usually associated with a state actor. Though it is generally placed in the non-state category, this creates a unidimensional picture and leads to a partial understanding of its characteristics and patterns of behavior. By recognizing the multiple identities of actors of this kind and a strategy that is not always coherent because different identities and commitments are being juggled, we could have a broader understanding of their development and current characteristics, not only historically and descriptively, as usually happens, but in a manner that reveals deeper layers of discourse and practices. ISIS is an example of a non-state actor that does not accept the existing order and aspires to change it, but at the same time, acts in a state-like manner in attempting to manage a civilian infrastructure for the population under its control. It is still difficult to measure its achievements. However, it would appear that compared to other similar actors in the region, ISIS has taken the first step in its attempt to reshape borders in the Middle East, thus far by blurring the border between Iraq and Syria.

At present, it is not only violent armed organizations that are attempting to redefine the Middle East's borders, but also other non-state actors with an ethnic or tribal-familial motivation. The Kurds in Iraq are a conspicuous example of this trend.

These developments raise the question whether and to what extent theories and concepts in international relations can help us understand

the non-state situation and its trends. As noted, the approaches examined in this article—realism, liberalism, and constructivism— give a different weight to the non-state phenomenon. The strengthening of these actors as well as their influence on the international system led the approaches of the 1970s to refresh their principles. In fact, the "neo" approaches have given greater weight to these actors than in the past. Nevertheless, the common claim that the theories, primarily realism and liberalism and their development, largely preserve the state system that is composed of sovereign states, is still valid.[36] These theories reinforce thinking from a certain field and thus limit the possibility of combining knowledge from different disciplines (history, geography, sociology, and the like). Another problem is connected to the focus in these approaches on one level of analysis (for example, a system or a state) and an excessively dichotomous view of the types of actors (state or non-state). So too, the theories assume that it is the structure and system that dictate the interaction and not the choices of the actors themselves.[37] Therefore, approaches in international relations lead to a certain reductionism and ignore complex phenomena that combine different levels of analysis and interaction, such as the case studies examined.

Despite the limitations of the comparison, it appears that constructivism is more suited for an analysis of phenomena characteristic of the current Middle Eastern order, especially because it is pluralistic and dynamic and because it recognizes the ideological component and ideological concepts as shaping the choices of actors.

On the theoretical level, this study recommends that social scientists, when studying phenomena in the international system in general and the Middle East in particular, apply the paradigms of international relations more horizontally than vertically, that is, that they derive from them middle-range theories that will help to explain and contend with complex phenomena. It is important to adopt approaches that recognize the multiple dimensions of phenomena, the different types of actors, and the factors from different levels of analysis, which explain processes and not just results. It appears that the time has come to rethink the total application of a certain paradigm to a social phenomenon and to think about a flexible use with a more fluid transition from one paradigm to the next. Otherwise, the gap between the complex situation and the theory that subsumes it will continue to grow deeper.

On the practical level, states in the region would do well to become accustomed to the non-state environment – which will apparently become increasingly common in the Middle East – inter alia, by adopting non-state thinking. This statement is more acceptable in its military contexts. The past four decades have proven that Israel's adversaries have gone from states to non-state actors and have led to an improvement in thinking and strategy for dealing with them. It would appear that the time has come to expand military thinking to other areas (including the political, diplomatic, and legal). These could assist us in understanding and better coping with non-state phenomena in the Middle East. They could even enable us to think in terms of collaborations and alliances with non-state actors with regional influence.

Notes

1 Fund For Peace, "Fragile States Index 2014," http://ffp.statesindex.org/rankings-2014.

2 The approaches chosen actually represent two competing paradigms: the realistic and the liberal belong to the utilitarian and rationalist paradigms, respectively, while constructivism is associated with an interpretive paradigm.

3 Daphne Josselin and William Wallace, eds., *Non-state Actors in World Politics* (London: Palgrave Macmillan, 2001), pp. 3-4.

4 National Intelligence Council (NIC), "Nonstate Actors: Impact on International Relations and Implications for the United States," August 2007, http://fas.org/irp/nic/nonstate_actors_2007.pdf.

5 Jason Bartolomei, William Casebeer, and Troy S. Thomas, *Modeling Violent Non-State Actors: A Summary of Concepts and Methods* (Colorado: United States Air Force Academy, Institute for Information Technology Applications, 2004), p. 7.

6 Phil Williams, *Violent Non-State Actors and International and National Security: International Relations and Security Network* (Zurich: Federal Institute of Technology, 2008), p. 8.

7 Hans Morgenthau, *Politics among Nations: The Struggle for Power and Peace* (New York: Alfred A. Knopf, 1948), p. 21.

8 B. Hocking and M. Smith, *World Politics* (New York: Harvester Wheatsheaf, 1990), p. 80.

9 C. Archer, *International Organizations*, Second Edition (London: Routledge, 1992), p. 85.

10 James Rosenau, *Along the Domestic-Foreign Frontier* (Cambridge: Cambridge University Press, 1997); R. O. Keohane and J. S. Nye, eds., *Transnational Relations and World Politics* (Cambridge: Harvard University Press, 1971).

11 Ibid.

12 R. O. Keohane and J. S. Nye, *Power and Interdependence*, Second Edition (Glenview Illinois: Scott, Foresman, 1989), pp. 24-25.
13 Keohane and Nye, *Transnational Relations and World Politics*, p. 332.
14 R. W. Mansbach., Y. Ferguson, and D. Lampert, *The Web of World Politics: Non-State Actors in the Global System* (Englewood Cliffs, New Jersey: Prentice Hall, 1976), pp. 273-76.
15 M. Hollis and S. Smith, *Explaining and Understanding International Relations* (Oxford: Clarendon Press, 1992), pp. 36-37.
16 Kenneth Waltz, *Theory of International Politics* (Michigan: Addison-Wesley, 1979), pp. 69-72.
17 Ibid., p. 93.
18 Emanuel Adler, "Seizing the Middle Ground: Constructivism in World Politics," *European Journal of International Relations* 3, no. 3 (1997): 319-63.
19 Alexander Wendt, "Anarchy Is What States Make of It: The Social Construction of Power Politics," *International Organization* 46, no. 2 (1992): 391-425.
20 Marc Lynch, "Al-Qaeda's Constructivist Turn," *Praeger Security*, 2006, http://www.marclynch.com/2006/01/17/al-qaedas-constructivist-turn.
21 The neoliberal approach is more an economic approach advocating minimal state intervention, and only in time of need, to ensure the right to private property, the rule of law, and institutions that allow the functioning of markets and free trade. According to this approach, reducing the role of the state and transferring responsibility to the individual will ensure growth and freedom.
22 Max Weber, *The Theory of Social and Economic Organization* (New York: Free Press, 1964), p. 154.
23 Michael Mann, "The Autonomous Power of the State: Its Origins, Mechanisms, and Results," *European Journal of Sociology* 25, no. 2 (1984): 112-13.
24 Naim Qassem, *Hizbullah: The Story from Within* (London: Saqi Books, 2005), pp. 200-205.
25 This abstract is based on research conducted for a doctoral dissertation. Carmit Valensi, "The Growth of Hybrid Actors: The Case of Hamas, Hizbollah, and FARC" (Tel Aviv: Tel Aviv University, 2014).
26 Shimon Shapira, *Hizbollah between Iran and Lebanon* (Tel Aviv: Kibbutz Meuhad, 2000), p. 146.
27 Amal Saad-Ghorayeb, *Hizbollah al-Din wal-Siyasiyah* (Beirut: Dar al-Kitab al-Arabi, 2002), p. 45.
28 See, for example, Anisseh Van Engeland and Rachel M. Rudolph, *From Terrorism to Politics* (Burlington, VT: Ashgate, 2008), p. 5.
29 Benedetta Berti, "Armed Groups as Political Parties and Their Role in Electoral Politics: The Case of Hizballah," *Studies in Conflict & Terrorism* 34, no. 12 (2011): 942-62.

30 This idea was clearly presented on the organization's propaganda web sites. The Al Hayat Media Center has a video calling for the "end of Sykes-Picot." See https://www.youtube.com/watch?v=VjOGkPpafyo. The al-Atsam propaganda institute has a campaign called "Breaking Borders" (in Arabic). See https://www.youtube.com/watch?v=g4Xh2EPr6qM.

31 James Piscatori, *Islam in a World of Nation-States* (Cambridge: Cambridge University Press, 1986), pp. 47-49.

32 Abu-l-'Ala Mawdudi, "Nationalism and Islam," in *Islam in Transition,* J. L. Esposito, ed. (New York: Oxford University Press, 1982), pp. 94-95.

33 From a speech by Abu Bakr al-Baghdadi, YouTube, July 5, 2014, https://www.youtube.com/watch?v=VOORW63ioY0

34 A copy of the document can be found at http://www.almustaqbalnews.net/128495 (Arabic).

35 Yaron Friedman, "The Project to Dismantle States—Daesh Control," *Ynet*, June 12, 2014, http://www.ynet.co.il/articles/0,7340,L-4529767,00.html.

36 James Rosenau, *Turbulence in World Politics: A Theory of Change and Continuity* (Princeton: Princeton University Press, 1990), p. 37; R. W. Mansbach and Y. Ferguson, *Remapping Global Politics: History's Revenge and Future Shock* (New York: Cambridge University Press, 2004), pp. 110-12.

37 Amir Lupovici, "Me and the Other in International Relations: An Alternative Pluralist International Relations 101," *International Studies Perspectives* 14 (2013), pp. 238-39.

Critical Infrastructures and their Interdependence in a Cyber Attack – The Case of the U.S.

Harel Menashri and Gil Baram

The growing use of information technology, monitoring, and control through computerized control systems, together with the increasing dependence of the free market on products and services supplied through infrastructure (for example, electric power), have increased interdependency between infrastructures. Consequently, an attack on critical infrastructure is liable to have a decisive effect on the functioning of other infrastructures. The interdependence between infrastructures requires those involved in planning a cyber-attack as well as those involved in defending from such attacks to adjust to this reality and prepare accordingly. The article describes the existing models for analyzing interdependence between infrastructures, proposes an analytical framework for describing the interdependence and examines the possibilities at the United States' disposal should it decide to engage in a cyber-attack.

Key Words: critical infrastructure, interdependence, cyber-attack

Since the September 11, 2001 terrorist attacks, the U.S. administration has adopted a series of actions in order to improve security issues, including cyber security. As early as November 2002, President George Bush signed National Security Presidential Directive No. 16, directing government agencies, headed by the Department of Homeland Security (DHS), to develop

Dr. Harel Menashri is a fellow at the International Institute for Counter-Terrorism at the Herzliya Interdisciplinary Center.
Gil Baram is a doctoral candidate in the program for outstanding students in the Political Science Department at Tel Aviv University, and a researcher at the Yuval Ne'eman Workshop for Science, Technology and Security.

national guidelines determining when and under what circumstances the U.S. will be able to carry out cyber-attacks from its territory.[1] In February 2003, the White House published a document called "The National Strategy to Secure Cyberspace," portraying cyber security as a matter under the responsibility of the DHS. The purpose of the document was to provide "a framework for protecting the infrastructures that are essential to our economy, security, and way of life." The document contained a broad range of actions designed to protect the U.S. national security through the defense of its key critical infrastructures. The goal of this strategy was to create a working framework that would, for the first time, define priorities and instruct the various governmental authorities how to act in order to strengthen their cyber defense.[2]

Widespread activity in this sphere also took place during President Obama's term in office, with an emphasis on the importance of the cyber threat in the context of the publication of the National Security Strategy in May 2010, as well as publication of the International Strategy for Cyberspace in May 2011, which lay the foundation for clear methods of action in dealing with the cyber threat. This was reflected in a Pentagon statement according to which when warranted, the United States will respond to hostile acts in cyberspace as it would to any other threat to the country.[3] In November 2014, the director of the National Security Agency (NSA) issued a warning about Chinese and "two or three other countries'" ability to damage critical infrastructure in the U.S., including electricity, aviation, and financial systems, through cyber-attacks.[4] In January 2015 President Obama asked Congress to pass legislation on the subject of facing the growing cyber threat.[5] These official statements and others indicate that cyber security and defense of critical national infrastructures have been on the U.S. decision-makers' agenda for almost two decades, and they are of considerable importance to the American administration.

The interdependence between infrastructures requires those planning a cyber-attack to consider the connections between the infrastructures that they plan to attack and other infrastructures, including those in the target country, in the attackers' country, and in other countries in order to avoid damage that will affect the infrastructure in their own country, as well as avoid damage to other infrastructures which is liable to be considered a war crime. The parties defending infrastructures must study and map the connections and interdependency between the various infrastructures,

provide for redundancy, and prevent a domino effect in the event of damage to one of them.

The purpose of this article is to propose a general framework for describing the interdependence between infrastructures, and to examine the possibilities at the U.S.'s disposal in conducting a cyber-attack. The article is constructed as follows: first, the existing models for analyzing states of interdependency between infrastructures are presented and described. It should be noted that even though these models are not new, they are very relevant to the present time, because almost no changes have occurred in the development and operative characteristics of most of the infrastructures over the past decade, a fact that constitutes a significant weak point, and makes them an easier target for cyber-attacks. Next, the article analyzes the mutual interdependency between infrastructures in the case of the U.S., and assesses the consequences that decision-makers in the U.S. must take into account, in addition to considerations such as beginning a campaign that will jeopardize American infrastructures.

An Attack on Co-Dependent Infrastructures

There is a link between the infrastructures in industrialized countries like the U.S. and the infrastructures in other countries, and at times they are dependent upon each other. The global economy and trade relations between countries rely on electronic communications that facilitate ties, commercial transactions, and transmission of information and knowledge around the world at almost the speed of light. In many countries, technological progress – mainly in the field of communications – enables giant international corporations to operate and maintain this infrastructure. American corporations also invest resources in the infrastructures and economies of other countries. The global economy depends on a constant supply of energy resources. For example, the Chinese economy depends on a supply of energy resources from the Persian Gulf.

The introduction of critical infrastructures into all industrial sectors (such as water, energy, transportation, and the like) is accompanied by major long-term investments. Construction of these infrastructures takes many years, and therefore the management, monitoring, and control system for these infrastructures (Supervisory Control and Data Acquisition, SCADA), which are based on programmed industrial controllers, are infrequently revised, unlike the prevailing frenetic and rapid time spans in the current cyber world. Accordingly, an assessment of the durability of infrastructure

systems is also based on conservative models which, despite the time that has passed since they were developed, are still valid and relevant.

According to the model set forth by Steven Rinaldi,[6] when countries share common infrastructures, for example electricity, water, and gas, an attack on the infrastructure of one country is liable to affect the infrastructure of the other country. Clearly, the U.S. infrastructures and economy are liable to suffer devastating damage if the infrastructure and economies of other countries linked to them are attacked.

Together with the interdependency between countries, there is also mutual interdependence between infrastructures within the same country. An attack on one infrastructure is liable to cause a chain reaction or domino effect, in which infrastructures are damaged one after another. For example:

1. Infrastructure that produces electricity depends on a resource supplied through other infrastructure, such as oil or gas. An attack on the oil or gas infrastructure will affect the electrical infrastructure.
2. An attack on financial infrastructures, such as a stock exchange and banks, is liable to damage other infrastructures that require a flow of cash for their activity. Obviously, other scenarios of damage to public order due to economic problems are also possible.
3. An attack on the U.S. railway infrastructure is liable to have a severe effect on trade in the U.S. and its economy, and could cause food shortages in various regions throughout the country within a few days.
4. An attack on power plants or the transforming of electricity during peak periods is liable to cause a chain reaction in which additional power plants stop functioning. Such an event occurred in the U.S. in August 2003, when an operational malfunction in a transforming plant resulting from negligence caused a crash in electricity production and supply systems. This was the worst power blackout in the history of North America – residents of the northeastern U.S. and Canada were cut off from the electricity grid for many hours and even days.[7]
5. An attack on electrical infrastructure is liable to have an immediate effect on other national and municipal infrastructures: hospitals, industrial production, and damage to communications and transportation systems, mainly on land, but also certain air transportation systems.
6. An attack on the traffic system in a busy traffic lane will cause a transportation chain reaction that will affect other systems whose activity depends on transportation infrastructures.

In the process of planning an attack on an enemy's critical infrastructure, the attacker must consider precisely how the target infrastructure is linked to other infrastructures, and how these infrastructures depend on each other. It is sometimes possible to consider the possibility of attacking the target infrastructure by means of an attack on other infrastructure connected to it: a weak point may be found in the systems of the connected infrastructure that will make it easier and more convenient to attack.

The theoretical methodology used to assess the interdependence between critical infrastructures is displayed in Figure 1 below, taken from a study by Gillette, Fisher, Peerenboom, and Whitfield.[8] The diagram demonstrates the links and interdependence between the critical infrastructures, with electrical infrastructure in the center linked to all the others, and all of them dependent on its proper operation.

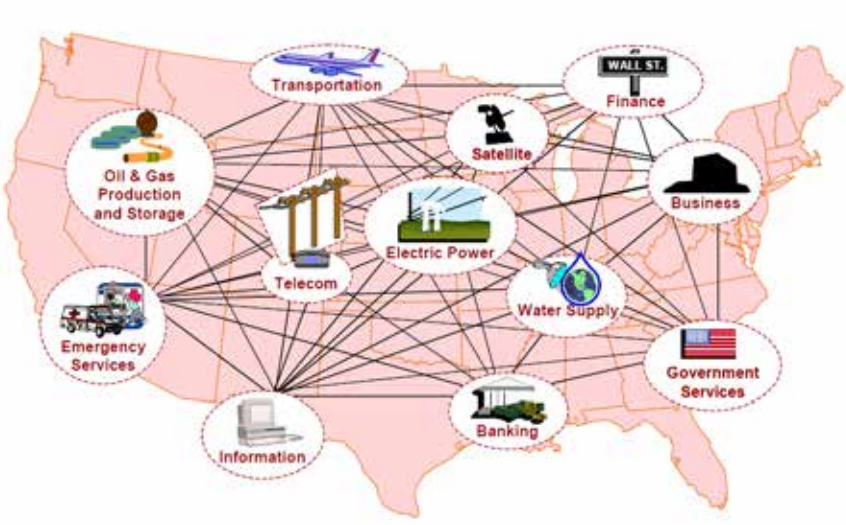


Figure 1: Critical Linked and Interdependent Infrastructures in the United States

Source: Gillette, J., Fisher, R., Peerenboom, J. and Whitfield, R, *Analyzing Water/ Wastewater Infrastructure Interdependencies* (Lemont, Illinois: Infrastructure Assurance Center – ANL, Argonne National Laboratory, 2006).

Addressing Interdependence between Infrastructures

The issue of mutual interdependence between critical infrastructures in the U.S. is mentioned for the first time in 1998, in Presidential Decision Directive No. 63, which deals with protection of infrastructure.[9] Two events influenced the publication of this directive: the attack on the government building in Oklahoma on April 19, 1995 and the activity of the scientific task team on the subject of information warfare in 1996.

Presidential Decision Directive No. 63 stated, for the first time, that the national and economic security of the American people depended on critical infrastructures and the information systems supporting their proper operation. In order to ensure their reliability and protection, committees were established for every infrastructure sector, while the appropriate federal authority was instructed to investigate problems relevant to the sector. The activity of these committees focused on protecting the information systems against hostile penetration, i.e. computer attacks, liable to cause a failure in the essential infrastructures.

Essential infrastructures can be roughly divided into two main categories:

1. Infrastructures whose activity relies solely on information technology (IT), referring to most financial infrastructures;
2. Infrastructures operating through SCADA systems. These special control, monitoring, and management systems are typical of critical national infrastructures, such as electricity, water, gas, fuel, communications, and transportation. The information in these systems is sent from the controllers deployed in the field to the control center, and from there to the operational systems in real time. The systems use sensors providing real-time information on their status, used for controlling and implementing operational changes. For example, in a pipeline transporting material from a container to a facility that uses the material, the sensors provide a real-time status of the amount and volume of material in every part of the system.

One suitable model for describing the behavior of the essential infrastructures and the interdependence between them is based on the definition of infrastructure systems as Complex Adaptive Systems (CAS). These systems are complex, because they are diverse, and contain a large number of interlinked components. They are adaptable, because the capabilities of the components and their decision rules change over time in response to information from other components, and to external intervention. The term "CAS" was coined in 1994 at the interdisciplinary

Santa Fe Institute (SFI), by John H. Holland, physicist Murray Gell-Mann, and others in 1994. Additional examples of complex adaptive systems are the stock market, insect and ant colonies, climate systems, the human brain, and the immune system.

A General Framework for Describing the Mutual Interdependence between Infrastructures

In 2001, Rinaldi, then Chief of the Modernization and Technology Issues Branch, United State Air Force Quadrennial Defense Review Office, proposed a general framework for describing the mutual interdependence between infrastructures. In a joint study with other researchers, CAS systems were identified, and six spheres of reference were presented, according to which data could be provided concerning the mutual interdependence between infrastructures (see Table no. 1). The subject presented in the document has constituted the basis for theoretical and applied research in this field ever since.[10]

Table 1: Dimensions for Describing Infrastructure Interdependencies
(Rinaldi et al., 2001)

Types of Interdependencies	Type of Failure	Infrastructure Characteristics
· Physical Interdependency · Geographic Interdependency · Cyber Interdependency · Logical Interdependency	· Common cause · Escalating · Cascading	· Spatial (Geographic) · Temporal range · Operational factors · Organizational considerations
State of Operation (of the Infrastructure)	Infrastructure Environment	Coupling and Responsive Behavior
· Normal · Stressed/Disrupted · Repair/ Restoration	· Public policy · Legislation and regulation · Business-economic factors · Public health and safety · Political and social factors · Technology and Security	· Power of the coupling: · Tight/loose · Order of the coupling: Direct/indirect · Complexity of the coupling: Linear/complex

According to the document, the first sphere of reference that can mark mutual interdependence between infrastructures is the type of dependence. Mutual interdependence is defined as a bi-directional link between infrastructures, through which the state of each of the infrastructures is affected by the state of the other. The bi-directional characteristic is likely to be multi-channel, meaning that one infrastructure is dependent on a second infrastructure in a given channel, while the second is dependent on the first in a different channel. The interdependence between infrastructures is defined as a uni-directional link when the state of one of the infrastructures affects the state of the other infrastructure, but the second does not necessarily affect the first; for example, a communications system depends on the electrical system for the supply of electricity to the activity of its components, but the electrical infrastructure may not be dependent on the activity of the communications system.

There are four distinguishable types of interdependencies:

1. *Physical*. Two infrastructures are physically dependent when each depends on a physical product of the other. In this situation, a physical product from one infrastructure is a physical input for the other. For instance, a coal-powered power plant provides power for a railway network that transports the coal to the power station.
2. *Geographical*. Infrastructures are geographically dependent if a local environmental event can cause a change in their state.
3. *Cyber*. When the state of an infrastructure is conditioned upon information broadcast through the information or communications infrastructure. For example, production of electricity is conditioned, among other things, on information transmitted about the consumers' consumption of electricity.
4. *Logical*. Two infrastructures are logically dependent when the state of one infrastructure depends on the state of the other through some mechanism that is not a physical, geographical, or computer link. In principle, dependence of this type is created through decision-making processes made by the human factor, for example through political, legal, regulatory, or business measures (such as mergers).

The second sphere of reference that can indicate mutual interdependence between infrastructures is the type of failure. Three types of failure can affect mutually interdependent infrastructures:

1. *Common cause failure*. Disruption in two or more infrastructures simultaneously affected by a common cause. Example: failures in various infrastructures caused by weather damage.
2. *Escalating failure*. Failure in one infrastructure affects an independent disruption in another infrastructure. One example is the recovery time for repairing a failure in an infrastructure in which a component breaks down due to the unavailability of another infrastructure, delaying the delivery of spare parts.
3. *Cascading failure*. Disruption in one infrastructure will cause disruption in several other infrastructures. The most prominent example is the blackout in August 2003 in the U.S. and Canada, when a failure in the supply of electricity caused stoppages in communications and the supply of water, which in turn brought air traffic and other activity to a halt.

The third sphere of reference that can indicate mutual interdependence between infrastructures is the infrastructure characteristics. According to the above table, there are four distinguishable characteristics.

1. *Spatial scales*. This includes two aspects: the internal structure of the infrastructure itself, and the geographical deployment of the infrastructure.

   The internal structure of the critical infrastructure consists of several levels. A part is the smallest distinguishable component in analyzing the system; a unit is a collection of functionally linked parts, for example a generator; a sub-system is an array of units, for example a secondary cooling unit; and a system is an assembly of sub-systems, for example a power station. A complete collection of similar systems is an infrastructure: all the generators, cooling units, and power stations, together with additional parts, units, sub-systems, and systems, make up the electrical infrastructure.

   An interdependent infrastructure is the linked architecture of infrastructures and environment. The geographical deployment of the infrastructure can also exist on several levels: municipal, for example a municipal water supply; regional, such as regional electrical systems; national, including transportation systems; and international, including communications and financial systems.
2. *Temporal range*. In operating infrastructures, there is a very broad span of temporal ranges, varying from fragments of seconds (in operating electrical systems, for example) to hours (in water, gas, and traffic systems), to years (upgrading infrastructures and expanding capacity,

for example). This aspect is related to the power of the coupling (close or loose, as explained below) between infrastructure characteristic, which affects the relevance of the analysis. For example, in analyzing the course of a sudden failure in the electrical system, rapid processes, such as mutual computer interdependence, whose temporal ranges vary from seconds to hours, can be critical for an analysis. This is true mainly when SCADA systems and Energy Management Systems (EMS) are involved. Slower processes, such as transporting coal to power stations by rail (on a scale of weeks), legislating new energy laws (years), or construction of new power stations (years to decades) are irrelevant to an analysis relating to temporal ranges of a few days.

3. *Operational factors*. This component affects the response of infrastructures when they operate under stress or disturbance. The operating elements are closely related to security and risks. They include operational rules, training operators, backup systems and system redundancy, bypasses in an emergency, continuity plans, and plans for security policy, including implementation and enforcement.
4. *Organizational considerations*. This is an important factor in the behavior of an infrastructure. It includes the effects of globalization, international ownership, regulation, government ownership versus private ownership, policy and organizational motivation, and the regulatory environment. These organizational aspects are likely to prove key factors in determining the operational characteristics of infrastructures, and have marked consequences for security and avoidance of risks.

The fourth sphere of reference that can indicate mutual interdependence between infrastructures is the operational state of the infrastructure. This is a continuity of different behaviors during routine operational states, varying from states of peak activity to low activity, times of pressure, when disruptions are discovered, or when repairs and renovations are taking place. The state of activity of a unit, sub-system, or system during a failure affects the extent and duration of the disruption and the damage to the provision of the service provided by the infrastructure. For example, the effect of events during times of peak demand for electricity (or gas, water, telephony, or at times of heavy traffic) will be different than the effect of the same events occurring when consumption is low.

According to the table, the fifth sphere of reference for assessing the mutual interdependence between infrastructures is the environmental sphere. Infrastructures operate not only through input, output, and

operational states; they operate in an environment influenced by other infrastructures. The infrastructure environment is the framework in which the infrastructure owners and operators set targets, create value for systems, simulate, and analyze their activity, and make decisions that affect their structure and activity. The table mentions several groups:

1. *Public policy*. This involves federal energy policy, security policy, economic policy, policy in response to disasters, and the policy that defines the areas of jurisdiction. The decision made by the American Federal Communications Commission (FCC) not to regulate the services of Internet providers, which had a substantial impact on the design and growth of communications infrastructure,[11] can be cited as an example of such a policy.

   Decisions about government investments are another important factor in public policy, affecting the environment in which infrastructures operate. Some examples of this are federal investments in defense technologies, computer networks, and satellite communications, on the basis of which comprehensive commercial infrastructures were developed.
2. *Legislative and regulatory factors*. These are also part of public policy, but due to their great importance, they should be addressed separately. Legal and regulatory aspects directly affect the activity of infrastructures. Regulated infrastructures operate under a tighter system of constraints than infrastructures that are completely free of regulation. Laws that place legal responsibility for the disclosure of private, medical, and banking information illustrate this issue. Other laws are likely to affect the structure of infrastructures, for example legislation requiring that communications services be provided.
3. *Business-economic factors, opportunities, and risks*. These are important forces that shape the environment in which infrastructures operate. Owners make business and structural decisions affecting the characteristics of their activity according to these factors. Information technology developments, government supervision or deregulation, and mergers are three factors with a major influence on the business and economic characteristics of the infrastructures environment.
4. *Public health and safety*. Legislation and regulation aimed at protecting human life, property, and public health and safety have a direct impact on the activity of infrastructures and their interdependence. For example, environmental protection legislation in California sets stringent standards

for pollutant emissions from power stations and for reducing air pollution and other health effects. This regulation directly affects operational decisions concerning the construction of new power stations that use new technologies, the choice of SCADA systems and other electronic systems, and the types of fuel that they use. These decisions affect the mutual interdependence created between the infrastructures.

5. *Political and social factors.* These factors drive markets and choices, and constitute a basis for determining the necessity for laws and regulations, the level of providing services, the extent of protection, and the level of its implementation. The international, social, and political forces and interests also shape the infrastructure environment, since many of the infrastructures have become international. For example, the American electricity infrastructure is now merged with the Canadian electricity infrastructure. Other international infrastructures include communications, fuel, and gas. Political issues affecting processes include producing electricity from water in the northwestern Pacific Ocean, non-American ownership of American communications infrastructure, etc.
6. *Technology and information security*. Security failures in one infrastructure raise the level of risk and have a negative impact on security at other infrastructures. For example, when a municipal water system is powered by the local electricity grid, a successful attack against the electricity grid SCADA system, the water supply system is liable to suffer from interruptions. Security of the water system is a result of the level of security in the electricity supply system, and the same is true for a disruption or failure.

The sixth sphere of reference for assessing the mutual interdependence between infrastructures is coupling and responsive behavior. Three topics are distinguishable in this sphere.

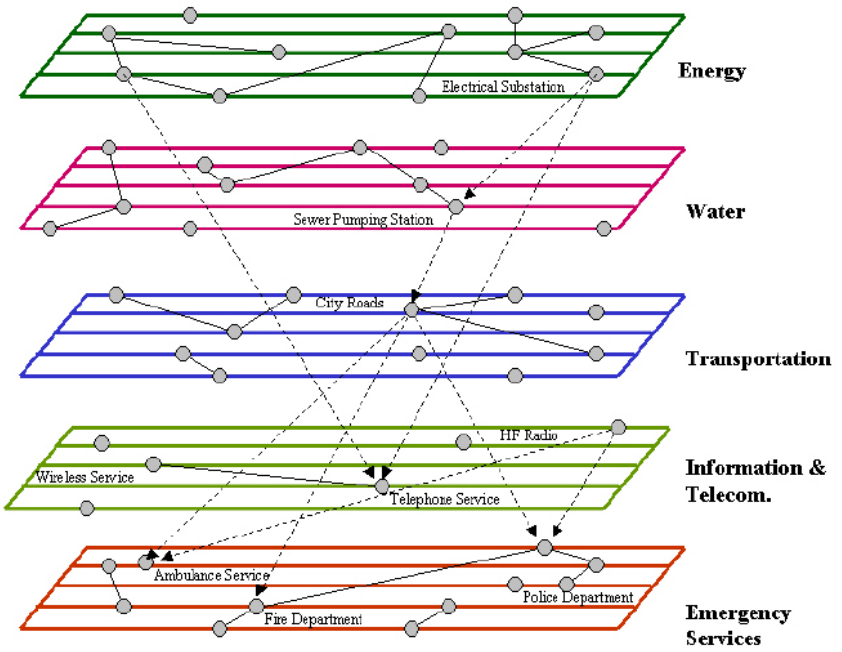
1. *Power: Tight or loose.* Tight coupling refers to infrastructures that are very dependent on each other. An interruption in one infrastructure is immediately linked to an interruption in the other infrastructure. One example of such a situation is a power station that runs on natural gas and the pipeline through which the natural gas flows. This coupling is especially close if there is no local gas reservoir, and if the power station cannot switch to using an alternative fuel source. In this situation, an interruption in the supply of natural gas will immediately cause an interruption in the production of electricity. Loose coupling exists when the infrastructure is relatively independent, and the state of one

infrastructure has almost no effect on the state of the other infrastructure. For instance, a coal-fueled power plant that usually has enough coal in storage for two to three months of operation, and the railway network used to transport coal to the plant. A temporary interruption in the coal supply does not immediately affect the functioning of the power station.

2. *Order: direct or indirect*. Direct coupling occurs when one infrastructure is directly connected to a second infrastructure. Indirect coupling is when the second infrastructure is connected to a third infrastructure; in this situation, the first infrastructure is connected to the third infrastructure through the second infrastructure, and the third infrastructure is therefore connected to the first infrastructure by indirect coupling. For example, an interruption in the supply of electricity will cause problems in the production of natural gas. That is direct coupling; further along the chain, enterprises that need natural gas for their operation will be affected, and that is indirect coupling between the supply of electricity and these enterprises.
3. *Complexity: linear or complex*. Linear mutual activity is part of a continuity of production or maintenance operations. At the same time, these operations, which are recognized and known, are likely to occur unexpectedly. Complex mutual activity is activity that is not part of the operational continuity, or is unplanned and unexpected, not in plain sight, and not immediately understood. For example, when a gas supply infrastructure is examined in isolation from other infrastructures, it can be regarded as if it were a linear system: gas flows from a given source to a gas stabilization plant, then through compression facilities and many gates, and eventually reaches the customer site. If the electricity production plant uses natural gas as a fuel source, and the electricity is used to operate the gas stabilization and compression plants, then the coupling between the gas and electricity infrastructures is in fact complex, not linear.

An example of a system of mutually interdependent infrastructures that affect each other can be seen in figure 2.

Figure 2: Mutual Interdependence between Municipal Infrastructures
(Pederson, Dudenhoeffer, Hartley & Permann, 2006)[12]



Source: Pederson, P., Dudenhoeffer, D., Hartley, S., and Permann, M., *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research* (Idaho National Laboratory – INL: August 2006).

The diagram shows how infrastrucures in the municipal sector are linked to each other, are mutually interdependent, and affected by each other. As shown here, the municipal emergency services, for example, police, fire department, and ambulances, are dependent on the communications and transportation infrastructures, which are in turn directly dependent on the energy infrastructures. There is also dependence between the transportation infrastructure and the water infrastructure.

The following table displays the power of the dependence bewteen the various infrastructures at three levels: high, medium, and low. For example, the food industry is highly dependent on the electricity, water, and sewage purification infrastructures, and only slightly dependent on the natural gas infrastructures. Health services are highly dependent on

the supply of electricity and water, and the electricity infrastructure is highly dependent on the supply of natural gas.

Table 2: The Power of the Interdependence between Infrastructures
(Pederson et al., 2006)

Sector		Energy and Utilities					Services	
	Infrastructure	Electrical Power	Water Purification	Sewage Treatment	Natural Gas	Oil Industry	Hospitals and Health Care Services	Food Industry
	Electrical Power		H		H	M		
Energy and Utilities	Water Purification	H				M		
	Sewage Treatment	M	L			L		
	Natural gas	L				L		
	Oil Industry	H	L					
Services	Hospitals and Health Care Services	H	H	L	M	H		H
	Food Industry	H	H	H	L	M	L	

H – High M – Medium L – Low

Based on what has been presented thus far, it seems that a direct attack on critical infrastructure is liable to indirectly, and perhaps even directly, affect other infrastructures in the attacked country, and possibly in other countries as well, including the country of the attacker himself. These attacks are also liable to cause or facilitate war crimes.

For instance, an attack on a country's natural gas transportation infrastructure is liable to also affect energy production in additional countries connected to this infrastructure, but are not a party to the conflict. The attack on energy production can later cause damage to critical services and infrastructures in the energy sector and other sectors, including fatalities, disruptions at hospitals and especially in emergency rooms, damage to the operation of traffic lights at intersections, and interruptions of activity at critical enterprises.

An attack on a system used to manage computer infrastructure of a banking system is liable to disrupt processes and money transfers, thereby

causing direct damage to international companies. These are likely to include companies from the attacker's country.

An attack on infrastructures that operate a large port – such as systems for loading cargoes on cargo ships or oil tankers – is liable to affect all global maritime traffic: the entry of ships into the port will be delayed, thereby disrupting the timetables of shipping lines throughout the world. Ports belonging to the attacker are also liable to suffer damage. This involves large-scale loss of income and economic damage.

An attack designed to disrupt the operations of traffic lights at key intersections in order to delay the movement of forces to the front is liable to cause delays and disruption in the movement of ambulances and emergency and rescue forces. An attack designed to disrupt railway operations is liable to have a negative impact on the movement of goods and food. In certain cases, it is even liable to cause derailment, thereby endangering human life.

In addition, conducting a cyber-war is likely to be greatly affected by the interdependency and links between the infrastructures. International ownership of an infrastructure will affect both the attacker and the defender. The defending parties are likely to take advantage of the fact that the infrastructure that they are protecting is owned by an international corporation that also controls infrastructures in the enemy country. They can convince the enemy not to attack, so that his infrastructures will not be damaged as a result of the attack. Attacking parties are likely to find such international ownership very useful; they can use it to collect information on the infrastructure that they are seeking to attack, and perhaps to implant hardware or software for use during a future attack.

The Effect of Interdependence between Infrastructures on American Cyber Activity

The infrastructures' elements and the mutual interdependence between them affect their adaptation and flexibility. The Complex Adaptive System model characterizes a system according to its ability to learn from past experience and adapt itself to future projections. Many factors contribute to a system's adaptability: availability, the number of alternatives to critical processes or products, continuity plans for emergencies, backup systems, training operational personnel, and the creativity of the human factor in disaster situations. Other factors liable to make infrastructure inflexible include restrictive regulation and legislation, social aspects, organizational

policy, and fixed network topologies.[13] A collection of flexible components has a better chance of responding well to disturbances and continuing to supply critical goods and services.

The American modus operandi involves a framework and cyber cover for every military scenario. The aim is to be able to neutralize the enemy's defense systems before warfare begins, while providing security for the American fighting forces' information and communications systems. In this way, in addition to attacking the enemy's command and control systems, critical elements will also be attacked, and the enemy's ability to operate battle systems will be damaged.[14]

The doctrine that was established by the U.S. requires attaining and maintaining accompanying cyber supremacy for every battle action, according to the enemy's capabilities. The American strategy advocates cyber control over the potential enemies' command, control, and logistics deployments in an attempt to decide the campaign before it begins, and in order to attack these deployments as necessary later in the campaign, should one erupt. According to the American concept, kinetic activities cannot exist without cyber activities; in other words, operations in which conventional capabilities are used (kinetic armaments) will always be accompanied by operational cyber-capabilities. On their own, kinetic battles are no longer sufficient to achieve objectives in the best and most effective way, and accompanying cyber action is therefore necessary. In addition, any offensive action in cyberspace will be accompanied by preliminary collection activity – also in cyberspace.

In order to implement this strategy, the U.S. Armed Forces have established a cyberspace operational deployment with defensive and offensive capabilities, based on cyber command capabilities (based on the superior capabilities of the National Security Agency). In addition to securing the cyberspace in which the military systems and technological support for the kinetic units operate, the tasks include defeating any potential enemy and maintaining American supremacy in cyberspace, while attacking the enemy deployment in this domain. Defensive capability plays a decisive role in a conflict and in victory in the asymmetric cyber environment, such as that experienced by the United State. For this reason, there is an acute need to create balance between attack and winning capabilities and deterrent capabilities and defense.

In October 2012, President Obama signed Presidential Policy Directive No. 20, classified top secret, which outlines the legal infrastructure and

procedures underlying U.S. cyber policy. The directive includes guidelines for implementing criteria for operations by all American government agencies in dealing with threats in cyberspace. The basic terms relevant to cyberspace are defined, such as offensive and defensive operations, defense of networks, hostile activity, influence operations, and information collection in cyberspace. The need to develop and use cyber tools is also emphasized as an integral part of national power and security.

As revealed by Edward Snowden,[15] in Presidential Policy Directive No. 20, President Obama instructed the force to assess, among other things, the effect of these actions on parties liable to suffer damage as a result of their actions. Any activity liable to harm human beings, cause significant damage to American interests or substantial property damage requires presidential approval.

It is clear from the wording of the directive that its authors were aware of the possibilities of collateral damage resulting from mutual dependence between infrastructures. In this framework, actions will comply with the laws of war, and actions liable to have cyber effects within the U.S. require presidential approval. An effort should be made to locate every party liable to be affected by the action – both within the U.S. and among the enemy parties; actions liable to have significant consequences (by implication, for both American and foreign infrastructures) require presidential approval in ordinary times (in an emergency, there is a different process). Cyber operations carried out in response to enemy operations should be minimal in order to avoid significant consequences; during the discussion about the action, the effect on American interests should be considered, including damage to communications networks and infrastructures. Possible responses to and consequences of cyber actions affecting American interests should be mapped and appropriate preparation should be made in advance of the action.

On May 27, 2013, it was announced that the U.S. Joint Chiefs of Staff intended to give the commanders of the Armed Forces authority enabling them to use offensive cyber weapons in response to cyber threats, without requiring approval from the National Security Council. The procedures were agreed as early as 2010, but their approval was delayed due to a legal dispute about the operative authority and the force of the response to cyber-attacks. Only after prolonged staff work was agreement on this issue reached.[16]

The superior American technological capabilities rest, among other things, in the fact that most systems used in cyberspace are operated by American-owned corporations, while the majority of the non-American companies have a rapport with the U.S. As a result, the U.S. is clearly dominant in all facets of cyberspace including attack capabilities, and can deter potential enemies through the threat of an attack on them.

A cyber warfare campaign raises new strategic and defense issues:

Commanders must have a good knowledge and understanding of the systems and the occasionally changing technologies. Familiarity with the technology makes it possible to understand the significance of cyber warfare events.

Cyber weapons are not very expensive, nor does training the attackers require large-scale investment. These costs enable terrorist groups and countries with limited means to take part in cyber-warfare.

The fighting takes place on critical infrastructures and information systems that in most cases are also used by the civilian population. When the infrastructures and information systems are the front, technicians become combat soldiers who are likely to play a decisive role.

In the event of an attack on an infrastructure, the links between the infrastructures and the involvement of the civilian market in management of information systems and infrastructures might cause a far-reaching chain reaction.

The absence of regulatory legislation and the absence of an international convention on cyber-warfare make it harder to determine what is permitted and what is forbidden in such a conflict. In particular, there is a lack of clarity about attacks on civilian infrastructures.

The information systems and defense realms have changed greatly in recent decades. The U.S. utilized cyber-capabilities in the 1991 Gulf War, and it is known that covert cyber activity by American intelligence agencies took place years earlier. It is absolutely clear that cyber warfare will be part of any future modern conflict, and can sometimes even have a dramatic effect that will decide the conflict.

In past wars, U.S. forces have been accused of excessive violence, sometimes without scruples about harming the innocent. Cyber warfare enables American forces to operate moderately and with restraint, while attempting to avoid harm to those not involved. Furthermore, American policymakers have created an image in which the features of American culture and democracy place strong inhibitions and constraints on the use

of cyber power in an attack. Nevertheless, until Snowden's revelation, the American administration emphasized primarily defense against cyber-attacks, and publicly accused China of conducting cyber-attacks against it. The information revealed indicated that at the same time that the U.S. was accusing China, it had itself conducted offensive cyber operations against the Chinese government. In view of this exposé, China publicly revealed what it called the American "double standard."[17]

This was not the only allegation of American hypocrisy; duplicity is an important element of the "soft power" strategy used by the U.S. in order to persuade other countries around the world to accept the legitimacy of its deeds, even when they do not coincide with official declared policy.[18]

The direct interdependence between infrastructures is likely to mean that an attack on a military information infrastructure will cause a chain reaction that will affect civilian infrastructures. Attacking a country's critical infrastructure is liable to affect infrastructures and production capacities in other countries connected to the attacked infrastructure, and which are not a part of the conflict of which the attack was part. For this reason, such an attack is liable to result in war crimes, and even to damage American interests. It appears that an attack on purely military targets, such as radar and anti-aircraft systems, or core non-conventional weapons production and distribution systems, will be easier to carry out.

The interdependence between infrastructures requires those planning an attack on foreign infrastructure to carefully examine the connections between the target infrastructures and additional infrastructures in the other country as well as in the home country. Such an examination will allow for an easier attack through targeting connected infrastructure in which the attacker has discovered a weakness.

In our opinion, the U.S. will engage in information collection, and will also attack the enemy when the latter operate against American infrastructures. Attack weapons with a non-devastating effect may be used against the infrastructures in enemy countries, as well as target-focused attack weapons that can bypass systems not included as targets, such as Stuxnet. American policymakers will continue to promote an international law on activity in cyberspace, or at least international regulation in the framework such as the Tallinn Manual (sponsored by NATO),[19] or in reliance on the Budapest Convention.[20] They will also try to find moral solutions for conducting a cyber-campaign in events in which human lives are liable to be lost.

Notes

1 Federation of American Scientists, National Security Presidential Directives [NSPD] George W. Bush Administration, http://www.fas.org/irp/offdocs/nspd/index.html; Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," *Washington Post*, February 7, 2003.

2 *The National Strategy to Secure Cyberspace*, President Bush, Washington. February 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

3 Lolita C. Baldor, "Pentagon Gets Cyberwar Guidelines," *Washington Times*, June 22, 2012, http://www.washingtontimes.com/news/2011/jun/22/military-gets-cyber-war-guidelines.

4 Patricia Zengerlensa, "Chief Warns Chinese Cyber-Attacks Could Shut U.S. Infrastructure," *Reuters,* November 21, 2014, http://www.reuters.com/article/2014/11/21/us-usa-security-nsa-idUSKCN0J420Q20141121.

5 Eric Chabrow, "Obama to Congress: Enact Cybersecurity Laws," *GovInfosecurity,* January 21, 2015. http://www.govinfosecurity.com/obama-to-congress-enact-cybersecurity-laws-a-7816; Nicole Blake Johnson, "Lawmakers Welcome Cybersecurity Talks with Obama," *FedTech*, January 21, 2015, http://www.fedtechmagazine.com/article/2015/01/lawmakers-welcome-cybersecurity-talks-obama.

6 Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine* (2001): 11-25, www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.

7 U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations" (April 2004), http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf..

8 Jerry Gillette, Ronald Fisher, James Peerenboom and Ronald Whitfield, "Analyzing Water/Wastewater Infrastructure Interdependencies," Infrastructure Assurance Center – Argonne National Laboratory. Lemont, Illinois (April 2006), www.dis.anl.gov/pubs/42598.pdf.

9 The White House, "Critical Infrastructure Protection Presidential Decision Directive/NSC-63," May 22, 1998, http://fas.org/irp/offdocs/pdd/pdd-63.htm.

10 Rinaldi, Peerenboom, and Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies."

11 Federal Communications Commission, "Preserving the Free and Open Internet," December 21, 2010, https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf.

12 Pederson, P., Dudenhoeffer, D., Hartley, S., and Permann, M. *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research* (Idaho National Laboratory: August 2000).

13 Network Topologies- the network configuration and the defined connections between its components. In the current example the network has a defined configuration and cannot change.

14 Menashri, H. "Integrating Cyber-Warfare into Different Types of Warfare: a Case Study: the US," PhD dissertation (Ramat Gan: Bar Ilan University, 2014).

15 "Obama Tells Intelligence Chiefs to Draw Up Cyber-Target List – Full Document Text," *Guardian*, June 7, 2013, http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text.

16 Zachary Fryer-Biggs, "Slowed by Debate and Uncertainty, New Rules Green Light Response to Cyber-Attacks," *Defense News* (May 27, 2013), http://archive.defensenews.com/article/20130527/DEFREG02/305270014/Slowed-by-Debate-Uncertainty-New-Rules-Green-Light-Response-Cyber-Attacks.

17 Jonathan Kaiman, "China Reacts Furiously to US Cyber-Espionage Charges," *Guardian*, May 20, 2014, http://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges.

18 Henry Farrell and Martha Finnemore, "The End of Hypocrisy - American Foreign Policy in the Age of Leaks," *Foreign Affairs*, November 2013, http://www.foreignaffairs.com/articles/140155/henry-farrell-and-martha-finnemore/the-end-of-hypocrisy.

19 Tallinn Manual Process, *NATO Cooperative Cyber Defense Centre of Excellence Tallinn*, Estonia. https://ccdcoe.org/tallinn-manual.html.

20 Convention on Cybercrime, *Council of Europe*, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp.

Considering Operation Protective Edge: Can Declaration of War Be Part of a Strategy to Offset the Asymmetry of the Israeli-Hamas Conflict in the Gaza Strip?

Kobi Michael and Ilana Kwartin

Three rounds of violence between Israel and Hamas since 2008 have not resulted in any change to the fundamental essence of the conflict. Israel is trapped in an asymmetrical conflict with increasingly intense violence, a reality in which Hamas manages to prove the "Paradox of Power": Israel's military strength becomes its weakness while Hamas' military weakness becomes its strength. Seeing Gaza as a state-like entity and declaring war on it may help alter public opinion, allowing for definition of clear goals and less engagement in dialecticism. Declaration of war could help lay a foundation of awareness more suitable to a change of the second degree, i.e., a change of the system, to distinguish from a change of the first degree, i.e., a change within the system. Analyzing the significance and implications of a declaration of war, this article does not rely on a case of an actual recent declaration; rather, it challenges conventional thought and may help in transforming the conflict by laying the foundation for rearranging the system, so as to manage the conflict at a lower level of violence and perhaps even end and resolve it.

Key words: Israel, Gaza, Hamas, declaration of war, asymmetrical conflict, awareness

Dr. Kobi Michael is a senior lecturer at Ariel University on Israel in the Middle East and Political Science and a senior research fellow at the Institute for National Security Studies.
Atty. Ilana Kwartin teaches at the Sapir Academic College Law School and is a PhD candidate in Gender Studies at Bar-Ilan University.

Military and Strategic Affairs | Volume 7 | No. 1 | March 2015

Introduction

"In war as in war," Maj. Gen. Giora Eiland wrote at the height of Operation Protective Edge, "only when we communicate at the level used between states and nations can we generate real deterrence or defeat the enemy when the next confrontation breaks out."[1] Stressing the importance of declaring war, Eiland explained that in all confrontations since 2006 Israel has fought terrorist organizations (whether Hizbollah or Hamas) with impressive skill and absolute military superiority, but with concurrent concern for non-combatants, including the supply of food, electricity, fuel, and medical care. As long as war is not declared, Israel is expected to fight and attend to humanitarian needs simultaneously.

Thirteen years after 9/11, U.S. President Barack Obama has yet to shape an effective strategy to fight Islamic terrorism. Indeed, some in the United States – Democrats and Republicans alike – believe the time has come for Obama to declare war on the Islamic State (ISIS).[2]

On July 7, 2014, Israel embarked on Operation Protective Edge in the Gaza Strip. It began as a focused aerial battle that to a large degree was forced on Israel. However, once it began, Israel chose to act in a way that facilitated preservation of its initial strategic interest: that Hamas remain the functional governing entity, accountable and responsible for the civilian population.

Israel's intention was to engage in a focused aerial campaign designed to cause massive damage to Hamas' military infrastructures in order to restore and maintain deterrence. However, in practice, Israel got caught up in the longest of the three recent preceding military engagements: the Second Lebanon War and the two operations in the Gaza Strip.

This operation, like the earlier ones, did not begin with a formal declaration of war. The operation expanded over time and lasted beyond initial expectations. The general feeling of most Israeli citizens, as well as that of military and security experts, was that this was a war,[3] and that the government "forgot" to declare war whether because of internal considerations or international ones. Although it ended with a ceasefire, the next round is only a matter of time.

Hamas' deployment of strategic capabilities in the form of naval commando units, UAVs and especially the use – and threat of use – of attack tunnels caused Israel to expand the operation by extensive deployment of ground troops. The operation lasted 51 days (which included several ceasefires violated by Hamas) and placed the IDF in a high-intensity military

confrontation that involved intensive friction with civilians in a densely populated, booby trapped urban setting, replete with terrorist tunnels.

The characteristics and intensity of the friction in the ground campaign, the operational and strategic necessity to destroy the tunnels, and the tremendous effort by Israeli forces to avoid Gazan civilian casualties greatly slowed the forces' progress and increased the level of risk to which they were exposed. But as time went by, the ground forces employed high-intensity firepower and, in many cases, required air and artillery support. This led to increased casualties amongst civilians and massive destruction of civilian infrastructures, inadvertently aiding Hamas' sophisticated media goals, and further eroding international legitimacy for a military move against the threats of terrorism and attack tunnels.

Operation Protective Edge was in many ways a war rather than an operation, but this is the third time that Israel, quite intentionally, has avoided issuing a declaration of war. This may have been inadvertent in the Second Lebanon War, which by any comparable parameter was fought at much lower intensity. This time around, the firepower and the levels of violence were much higher. In fact, the characteristics of Operation Protective Edge call into question the whole strategic concept that was formulated around the notion of low-intensity conflict. The operation also reflected the gap between the strategic view that the political and senior political echelons took about the nature of the operation on the one hand, and the military view at the operational and tactical levels on the other. It is safe to assume that this gap will have a significant role to play in the future as well.

Nonetheless, this was an asymmetrical war par excellence in which Hamas succeeded brilliantly in exploiting the advantages of urban guerrilla warfare. Hamas did not hesitate to use the civilian population as human shields and the urban sphere as a battlefield, thereby making it extremely difficult for the IDF, operating as a state-sponsored army on behalf of a Western democracy that subordinates itself to international laws of warfare. Hamas aimed at widespread damage to civilians and prepared to exploit the international media and sensitivity of the international community to horrifying sights of death and destruction (often distorted or completely fabricated and staged)[4] and used this to ostracize Israel, ramp up the delegitimization campaign against it, and use international criticism to limit Israel's ability to operate against Hamas.

This military campaign built on the advantages enjoyed by semi-state terrorist and guerrilla organizations in the reality of asymmetrical conflicts between states and semi-state entities. The nature of the arena and campaign greatly reduced Israel's scope of operations and strategic and operational flexibility. In fact, Israel's absolute military advantage was greatly eroded. Israel was unable to attain a sufficiently significant military achievement that might have been translated into a political objective and a new, long-term political reality. In fact, it was only during the operation's last week, after Israel bombed prominent symbols of Hamas's rule, especially the high-rise apartment buildings in downtown Gaza City, that Hamas changed its conduct. To borrow from Defense Minister Ya'alon, the turnaround in this operation – Hamas' agreeing to a ceasefire on Israel's terms – occurred only after Israel "removed the gloves" in the last week and dared do what it hadn't done before.

It is possible that in a conflict with greater symmetry between the warring sides, Israel may have had other methods of operation at its disposal by power of issuing a declaration of war, backed by international law. In addition, a reality of a declared war between two state entities shapes a very different public opinion on both sides of the conflict as well as in the international arena.

This article examines the theoretical significance of a declaration of war and its effect on the possibility of reducing asymmetry in a given conflict. The underlying assumption is that reducing asymmetry could allow Israel, as a state entity, greater spheres of strategic and operational flexibility that could increase the probability of maximizing military achievement, which could then be translated into a more significant political achievement.

Key Assertion

Three military operations against Hamas since December 2008 have failed to generate a change in the fundamental essence of the conflict. On the contrary, Hamas has only increased its strength, Israel's deterrence has waned, Israel's international reputation has been tarnished, and Hamas continues to leverage and maximize the asymmetrical aspect and establish the image of Israel's weakness vis-à-vis the ability to shape reality to serve its own strategic interests.

Relating to Gaza as a state-like entity and declaring war on it could allow Israel to set new rules into motion and create an alternate perception.[5] These could allow a reduction of the asymmetry and perhaps a greater military

achievement that may lead to greater damage to Hamas' military might, its political weakening, and its replacement by an alternative governing entity.[6] Such changes are likely to lead to a reconstruction of the Gaza Strip in a process of state building that would lay a possible foundation for resolving the conflict or at least attenuating it (e.g., demilitarizing the Gaza Strip for the sake of reconstruction at the hands of the Palestinian Authority instead of Hamas, strengthening the moderate elements in the region, resuming a political process, and creating a credible regional security regime).[7]

An operation such as Protective Edge, without a prior declaration of war, is liable to create dissonance and argument over the articulation of the strategic goal or objective (see the definition of Israel's strategic interest as noted at the beginning of this article).[8] A declaration of war is likely to help alter public awareness allowing for the definition of clear goals and less dialecticism. This could help reshape the battlefield, as opposed to changing the existing battlefield, while maintaining its formative rationale. Strategically speaking, declaration of war could help lay a foundation for perception more suitable to a change of the second degree, i.e., a change of the system, to distinguish from a change of the first degree, i.e., a change within the system.[9]

At first glance, it seems that a declaration of war contradicts the guiding rationale of conflict resolution strategies, but at times it is precisely the use of the paradoxical principle of strategy, i.e., acting completely contrary to linear intuition,[10] that allows the resolution of a conflict by means of its transformation.

The Theoretical Foundation

Given the limitations of the test case and without a formal declaration of war, this analysis is essentially theoretical, but to our understanding may serve as a conceptual expansion and challenge. The discussion will be divided into two parts: the first relates to the legal and ritual aspects of a declaration of war and to a new approach in the discipline of conflict resolution, known as "conflict transformation." We conclude this part by relating to asymmetrical confrontations and focus on the Israeli-Hamas conflict in the Gaza Strip. The second part of the discussion presents the major problem we seek to confront. We then lay the conceptual foundation and discuss the possible contribution a declaration of war can make to the transformation of an asymmetrical conflict.

Declaration of War: The Legal Aspect

In the past, a declaration of war[11] was considered a necessary legal act for engaging in war. The consequence of a declaration was an elimination of all diplomatic and commercial relations between two countries as well as the abrogation of all treaties between them. In the modern world, international legal implications of a declaration of war are less dramatic. In fact, since World War II, formal declarations of war have become quite rare.[12] In addition, there have also been mixed situations, creating ambiguity and confusion: war without fighting, fighting without war, military operations turning into wars, military interventions in third-party countries, using military force for limited duration and in limited location, and so on. Indeed, "one of the signs of the modern world is that the use of force has become commonplace whereas wars between nations have become rare."[13]

As a rule, international law places limits on nations' rights to use military force against others;[14] the United Nations Charter of 1945 prohibits the use of force in Article 2, Section 4, which states that "all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[15] The ban on the use of force is also a custom law that obligates non-U.N. members. Two exceptions to the ban on the use of force are a Security Council resolution permitting the use of force and engaging in self- and/or collective defense.[16]

According to Article 1 in the laws of war established in the 1907 Hague Convention,[17] "the Contracting Powers recognize that hostilities between themselves must not commence without previous and explicit warning, in the form either of a reasoned declaration of war or of an ultimatum with conditional declaration of war. The warning must come first − "previous warning" − rather than be retroactive. According to Article 2 of the convention, "the existence of a state of war must be notified to the neutral Powers without delay." The rationale for Article 1 would seem to be a prohibition on surprising the enemy with a war it did not expect. This rationale seems odd and not well-suited to the waging of any war as the element of surprise is one of the most important tools for achieving an advantage on the battlefield whereas a formal declaration of war is liable to undermine that advantage.

At present, some researchers and jurists posit that nations concede their right to resolve conflicts by means of a declaration of war because of the charters of which they are members.[18] Still, the question whether the

emergence of terrorist organizations and non-state players has neutralized that concession and restored the right to formally declare war, as was the case in the past, has yet to be fully resolved.[19] We assert that the determinative impact of a declaration of war as a ceremony is powerful and significant in its effect on any group of people, whether defined as a state, organization, non-state entity, or other.[20]

In Israeli law, Basic Law: The Government, Paragraph 40(a) indicates that the state can only start a war by virtue of a government decision. A government that decides to go to war must inform the Security and Foreign Affairs Committee of the Knesset "as soon as possible" and the prime minister must announce the decision to go to war to the Knesset plenum "as soon as possible."[21]

The above-mentioned Paragraph 40 ensures that the State of Israel does not begin a war without a decision by the government, which in turn is accountable to the Knesset. There may be several types of declarations of war, such as conditional, unconditional, comprehensive, or partial, but Israeli law does not distinguish among them. Moreover, Israeli law does not define the basis or the criteria according to which the government can declare war.[22]

We assert that the legal prism through which academics, military personnel, legal scholars, jurists, and policy makers are used to viewing declarations of war is too narrow and does not fully appreciate so complex and varied a phenomenon. We would like to reframe that view to say that a declaration of war contains great potential for a fundamental transformation of an asymmetrical reality and conflict characteristics. We therefore suggest an analysis of the phenomenon of declaration of war from a new point of view: an anthropological one.

Declaration of War: The Anthropological/Ritual Aspect

When referring to a declaration of war, Austin[23] defines it as a "declarative performative sentence." Kenny[24] posits that a declaration of war is a political act occurring in public "in the framework of asserting power relations."[25] The very act of a declaration creates a new situation even before any concrete act has taken place, and therefore the moment in time of the declaration represents both a beginning and an end, and has the power to generate a change to the current state of affairs. Austin[26] proposes a focus on the language and relevant contexts in which the words are spoken, and notice the power of those words.[27]

Kenny[28] explains that a political act, such as a declaration of war, structures the legal dialogue about the act rather than the other way around. Therefore, even though a declaration of war is anachronistic and may not be legally accepted in the modern era, it retains its "potential" effect at the political and transformative level.

In the past, war would be declared in a formal ritual representing a cutoff in time, separating two conditions: before and after; peace versus war. According to Van Gennep, a ritual, then, is a social phenomenon with symbolic value carried out with the proper, familiar ritual rules that are quite rigid and fixed and common to all of humanity, bearing a new important message: that of a change in situation.[29] Van Gennep stresses that the ritual has long-term effects as it is a political tool for generating change or transformation. According to Turner, rituals are held at turning points in life and through these rituals relations between people and social structures undergo a restructuring process.[30]

Handelman[31] emphasizes the importance of rituals as essential phenomena in which concentration of symbols with special contexts and meanings for a certain group of people occurs. Handelman stresses the ritual as a tool whereby one can generate a cosmological change and create a transformation in the world.[32] He explains that the form of the ritual shapes the ritual experience and creates the meaning imbued in it.

The ritual is noted for its repetition of contents and form. The ritual initiator enacts a pre-determined script; he does not act spontaneously. The behavior of the declaration is formal, symbolic, stylized and unique to the specific ritual. It is thereby set off from daily conduct.[33] The ritual has a constant order of its own and pre-determined, prepared documents attendant to it; the ritual is designed to create a certain state of awareness and emotion, a social obligation and/or commitment, and legitimacy for this change, and is therefore carried out in public with the message and its meaning clearly shared with the entire community and the world.[34]

Conflict Management and Resolution, Protracted Conflicts, and Conflict Transformation

Conflict resolution became an academic discipline following the Second World War.[35] The main theories in the field strive to find the generic organizing principles of conflicts, the reasons behind conflicts and their escalation, and the rationales and methods to manage and resolve them.[36]

Beyond the mainstream approaches in the field, the last decade has seen the growing acceptance of a new approach to protracted conflicts. Due to the tremendous difficulty in resolving this type of conflict and because of the high human, economic and political toll, a new approach stressing the rationale of Transforming conflicts was developed.[37] Conflict Transformation[38] is seen as an alternative paradigm to the traditional approach of conflict management and resolution,[39] and for many researchers represents a new development in the field[40] encompassing a more comprehensive approach than others.[41] According to this approach, the characteristics of the protracted conflict, especially its strategic and psychological blocks, do not allow its resolution. Therefore, there is need for a transformation of the conflict itself and the social and political system in which it is set.[42]

Unlike the conceptual world of conflict resolution, where the emphasis is placed on resolving conflicts in non-violent ways and escalation is viewed as negative and destructive, the Conflict Transformation approach presents a different vision: because the conflict is essentially based on interpersonal relations, at times it is precisely escalation that can lead to its resolution by means of a necessary structural change.[43] The desired transformation, according to this approach, is one that generates a "turnaround in the dynamics of conflicting interactions."[44]

Reducing the asymmetrical aspect of the conflict allows for changes in the rules of conduct and operation, which in turn make possible a spiral and circular approach – a non-linear rather than a linear approach – which is more relevant to dealing with the complexity of conflicts of this type. This approach seeks to help not only in settling the conflict or managing it, but to do something much deeper: "It points to the inherent dialectical process, the ability to transform the dynamic of the conflict and the relationship between the parties – indeed to transform the very creators of the conflict."[45]

Väyrynen points to a series of necessary transformations in the components of the conflict without which the conflict will be channeled into more violence and war.[46] Among the ways in which a conflict is transformed, the following are the most pertinent to our discussion:

- Context transformation: given that the conflict is rooted in social, regional and international contexts, a fact that contributes to its intractability, a change in context is necessary before any change can be made in the relationship between the parties.
- Structural transformation: the conflict comprises actors, contradictory objectives, and the parties' relationships. To the extent that the conflict

is fundamentally rooted in the structure of the relationship between the parties, a structural transformation (in the social-political sense and in the sense of the power structure of the parties involved) will help resolve the conflict. In asymmetrical conflicts, for example, a change in the asymmetrical reality between the powerful and the powerless party would represent a structural transformation.

Protracted Conflicts

Azar coined the term "Protracted Social Conflict (PSC)"[47] in reference to the Israeli-Arab conflict in the Middle East. Protracted conflicts, he claimed, incorporate ethnic (as well as religious) elements in conflicts between states, and are hostile and violent interactions spread over time during which there are war-like flare-ups at varying frequencies and intensities. In protracted and intractable conflicts, the entire population is involved, leading to national solidarity and identification. Despite periods of calm, it is impossible to point to an end, but one can use hindsight to isolate the process that led to the protracted conflict's end.[48]

Azar refers to violent episodes as part of the normal process of conflict and therefore developed a tool to examine volatility ranging from escalation to cooperation, calling it the "Normal Relations Range (NRR)."[49] Below we present a refinement of this tool as it relates to the conflict between Israel and Hamas.

The Asymmetrical Conflict: Attrition and Exhaustion as the Weapon of the Weak

In the past, most conflicts around the world were considered symmetrical in the sense of the statehood status of the parties involved. But in the last few decades the world of warfare has undergone a significant transformation and most violent conflicts conducted in recent years are characterized as asymmetrical conflicts, mostly between states with organized armies and sub-state entities in the form of terrorist or guerrilla organizations.[50]

In fact, more than 90 percent of today's conflicts are considered low-intensity conflicts[51] and are inherently asymmetrical. At present, conflicts are increasingly taking place between states and quasi-state entities, or between states and terrorist organizations (resembling protracted asymmetrical wars) [52] in which the asymmetry shapes the operating rationale of the actors.

The powerless side is the one that usually initiates the conflict; in some cases, it adopts the strategy of attrition[53] by means of terrorism and guerrilla

warfare designed to influence a decision made by the more powerful side, the state-entity, based on the understanding and knowledge that it cannot succeed in forcing a physical change.[54] This is true to organizations that operate with the help of locals who provide them with support and legitimacy, as well as refuge, and are willing to serve as human shields, all of which are designed to take advantage of the state's inability to act freely since it is committed to international law and moral norms. In such conflicts, there is no proven win-win outcome.[55] The new battlefield is densely populated by civilians and the new enemy is not an army. Non-state players make a point of blurring two prominent aspects of traditional warfare: the battlefield and the uniform.

The Israel-Hamas Conflict in the Gaza Strip

The State of Israel has a long history of fighting Hamas, but for the purpose of this article we focus on the period starting in January 2006 when Hamas was elected to the PA, and in particular since June 2007 when Hamas completed its forcible takeover of the Gaza Strip and became the exclusive sovereign (with the exception of the presence of the Islamic Jihad and other small terrorist organizations that challenge Hamas from time to time).[56]

Since then, Hamas, as a political and military movement, stands out due to its violent actions whose frequency, intensity, and duration are rising, as manifested in Operation Cast Lead (2008-2009), Operation Pillar of Defense (2012) and Operation Protective Edge (2014). If we examine Hamas' manifestations of violence through Azar's Normal Relations Range[57] model, we quickly discover a sharp, clear upward trend, to be discussed in the second part of this article.

Hamas' government in the Gaza Strip is solidly entrenched despite the attempts of different jihadist organizations to challenge it. Nevertheless, and although this government is supported by external parties such as Iran, Qatar and Turkey, the Gaza Strip, while operating like a state-like entity, has not developed into a functioning state entity. In fact, it is a failing state-like entity of which its very existence as such exacerbates the asymmetry of its conflict with Israel

The Gaza Strip as a Failing State-like Entity

The Gaza Strip is a semi-state entity; the characteristics of its existence are consistent with the four principles defining a state in the Montevideo Convention on the Rights and Duties of States.[58] On the other hand, it is

also a failing (semi-) state entity because it fulfills all the basic conditions defining failing states: a government that fails to provide for the needs of the local population, lack of legitimacy (its existence within Gaza strip itself is mostly coerced and the result of terrorist tactics), severe poverty, the lack of monopoly on the use of force (the very existence of terrorist organizations challenging the Hamas government to the point it is dragged into a military act such as Operation Protective Edge), and the government's violent, unchecked struggle for survival while violating every taboo on harming civilians.[59] It seems that this description applies to Hamas and the Gaza Strip in the wake of Operation Protective Edge.

The richer the rulers of failing states grow, the poorer and more exploited their citizens become. Personal human security is nonexistent in failing states, leaving citizens to fend for themselves. Because the state is incapable of providing for the basic needs of its citizens, organizations motivated by economic, social, political, ethnic, religious and/ or nationalistic interests enter the vacuum to exploit the weakness of the state and the people. They assume some of the responsibilities of the state, thereby advancing their own agendas and entrenching themselves in society.[60] This was the case in the Gaza Strip before Hamas' rise to power, facilitating seizure of power in the first place.

Failing states are not expected to vanish from the international arena in the near future, and clashes between established, functioning states and failing ones are inevitable.[61] These are, in fact, an updated version of asymmetrical conflicts, and therefore the test case before us is significant to local and international contexts alike.

One of the reasons for the inevitable clashes is the security threat created by failing states, because terrorist organizations, good at creating violence and terrorism against established, functioning states – even if they have no shared borders with the failing states and all the more so if they do – operate in and from them. Globalization, technology, widespread support in the form of financing from foreign sources, and accessibility to weapons of state, including WMDs, allow these terrorist organizations to operate cross-border terrorism, wreaking chaos at relatively low cost and with relative ease. Consequently, weak nations like Afghanistan can pose great danger to the national interests of strong nations.[62]

The Gaza Strip, as a failing semi-state entity, exports instability and insecurity to the region (Israel, Egypt and the PA) and forces the state players (Israel and Egypt) to use military violence to suppress terrorism

and threats. Nevertheless, the asymmetry is exploited by Hamas, which operates like an armed non-state player, especially in the Gaza Strip, in dictating the rules of the games, leading to a situation that reinforces the paradox of "the power of powerlessness" versus "the powerlessness of power."

Defining the Problem

Since Hamas seized control of the Gaza Strip and established its rule, the Gaza Strip has become a semi-state entity. Hamas institutionalized its military power, significantly improved military capabilities and infrastructures, developed the ability to manufacture rockets domestically and to build an underground network of attack tunnels, complete with command and control centers, weapons, and storage facilities. The features characterizing the Hamas state-like entity in the Gaza Strip are those of a failing state where the major effort exerted by the government is focused on its own survival.[63] These efforts are manifested in ongoing oppression of the population; especially those opposed to the regime, and in the constant preparations to confront the regime's external threat, in this case, the State of Israel.

The question at the heart of this article relates to Israel's ability to advance an arrangement of the sphere in a way that would serve its own strategic interests at a time when an asymmetrical reality is forced on it by a failing semi-state entity, dictating rules that do not allow Israel the opportunity to maximize its strength and advantages over Hamas.

The Basis of our Claim

The Israel-Hamas conflict is an intractable and protracted socio-religious conflict. These stem from the violent clashes between the sides; the intensity and frequency of the violence result in continual mutual attrition, with no end in sight. The intractability of the conflict also serves to perpetuate the psychological infrastructure[64] of the sides to the conflict and creates discrepancies that will not allow the conditions for a resolution.

1. The Israel-Hamas conflict intersects with other conflicts as it interlocks with other arenas and players,[65] a consequence of the Israeli-Palestinian conflict as it is affected by other conflicts and also affects them in turn.
2. The conflict comprises several simultaneous levels: it has complementary and sometime overlapping aspects, especially the military, political, ideological, cultural, religious, international and economic, but the most important one is the military, i.e., the violence aspect, which is

the main cause for the protracted nature of the conflict without there being an end in sight.

3. The Israel-Hamas conflict has a Normal Relations Range. Throughout the conflict there are upper and lower thresholds of violence. As soon as the upper threshold is reached, actors in the regional and international system attempt to contain the conflict and restore it to its normal range. Alternately, as soon as the conflict reaches the lower threshold, both domestic and external spoiler forces go into action to raise the level of violence and restore it to the normal range.
4. The level and scope of the violence are constantly on the rise. The Israel-Hamas conflict may be defined as a low-intensity asymmetrical conflict, but the intensity of the violence is on a constant upswing over time because of the military nature of the conflict.

An analysis of the conflict's features in recent years indicates that the Normal Relations Range is moving upwards as a block in terms of its values of violence and retaining the volatility in the level of violence within the developing relations range (see Figure 1). The rise in the level of violence develops with time, while the sides to the conflict gradually adapt to the new level of violence. It would seem that this structure will continue its escalation unless something is done. Therefore, we suggest a proactive move to stop the range from moving further upwards; a surprising transformative act could be just that proactive move. A declaration of war,

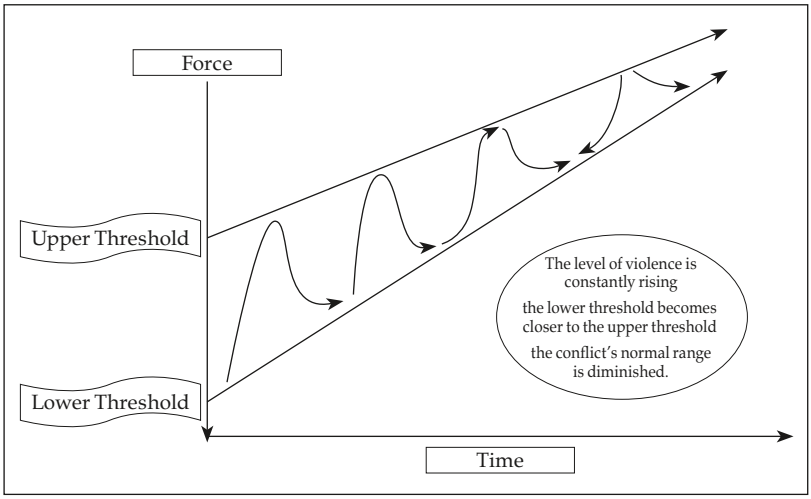


Figure 1. The Normal Relations Range in the Israel-Hamas Conflict

which has many advantages as well as certain drawbacks, could emerge as just that transformative act.

5. Resolving or managing the conflict at lower levels of violence requires a transformation of the conflict. In order to generate a structural transformation, it is necessary to change the power structure in the Gaza Strip, which means weakening Hamas and denying its relevance as a political player so as to allow the entrance of a different player (such as the Palestinian Authority) to take its place as the governing entity in order to rebuild the Gaza Strip and create a possible foundation for settling or mitigating the conflict. It is possible to weaken Hamas by causing significant damage to its military capabilities and infrastructures. Because Hamas' political power as the governing entity in the Gaza Strip is a direct consequence of its military might, damaging Hamas militarily would lead to damage to its political power.
6. A transformation of the conflict by means of a declaration of war could turn out to be a "fundamental surprise."[66] As such, it may disrupt Hamas' awareness at a very basic level (similar to a second tier change, a change of the system itself). A disruptive move of this kind could lead to an inversion in the dynamics between the sides and thus to a transformation of the conflict and a change in the developing trends of the conflict's normal relations range.

The Possible Contribution of a Declaration of War to a Transformation of the Conflict

A formal declaration of war places a shared responsibility on the authorities, leaving no room for vagueness. Furthermore, a declaration of war informs the entire nation that the lives of its citizens are about to change, and that they may pay dearly. Another important advantage stems from the fact that a declaration of war provides the executive with the political and moral authority – as well as the legitimacy – to conduct a war in the population's name and steer the military forces according to its considerations. Finally, a declaration of war leads to a binding paradoxical proceeding, which is likely to prevent unnecessary wars from breaking out.[67] The very act of declaring war may lead the other side to change its policy, and under these conditions a declaration of war becomes a type of deterrence.

By declaring war, the state shows that it is willing to do everything within its power, allocating all the required resources and changing its priorities accordingly.[68] Consequently, it can strengthen the potential for

deterrence while at the same time express a change in stances and belief, which may be seen as a direct consequence of a process of learning or, by extension, a manifestation of a leadership's readiness.[69] An example may be found in President G.W. Bush's declaration of war on terrorism in 2001. His declaration outlined the U.S. threshold and red lines, detailing the means the nation would use in defense of these interests. In addition to credibility, a declaration of war helps enlist the entire nation to support the declaration and can therefore be viewed as a collective act; hence its impact and advantage. It allows for the following:

1. *Abrogation of the dissonance of fighting the enemy while assisting it*. In the three operations Israel waged against Hamas in the Gaza Strip (2008-2009, 2012, and 2014), Israel continued to transfer– in practice via Hamas itself – raw materials, fuel, electricity and water, as well as humanitarian relief, which served to improve Hamas' endurance against Israel, reduce Gaza's domestic opposition to Hamas, and prolong the fighting.
2. *A shift of arena from population centers to a defined front*. At present, the biggest challenge the IDF must face – unlike the challenges faced by other Western armies – is fighting an armed entity that intentionally, cruelly and cynically sacrifices its civilians in order to present Israel as the demon, killing innocent bystanders.[70] A declaration of war, by its very definition, places the responsibility for the choice of fighting arena on the enemy.
3. *A prolonged hiatus and an exhaustion of the conflict*. The time factor is critical, and exhaustion exposes Israel's relative disadvantage as a developed Western nation compared to its enemy. Long and violent confrontations result in the depletion of Israel's forces, civilian and political exhaustion, and erosion of the citizens' trust in the state. The trust and cohesion in the government-military-civilian triangle[71] are its Achilles' heel: prolonging the conflict damages the Israeli economy and its citizens' morale. This stands in contrast to a non-democratic state or entity in which the regime's operations are independent of the trust of its (non-voting) citizens, free of accountability.
4. *A declaration of war would lead to fighting under conditions in which the IDF excels*. Most IDF units were formed and trained for high-intensity warfare and ground maneuvers, though in fact since 1982 they have been fighting guerilla forces.[72] Therefore, paradoxically, the transition to high-intensity fighting and ground maneuvers – consequences of

a declaration of war – would reduce the asymmetry and allow for the realization of the power of the state-sponsored army.[73]

5. *Legitimacy for the policy of war in general and the use of force in particular*. The bans on using force or limiting the proportionality of response in international law mostly apply to situations of confrontation rather than war. Subject to certain limitations, a nation at war has the legitimacy to defend itself at almost any cost. The military maneuvering room is greater under a declaration of war, because then the use of force is expected, permissible, and even imperative. When a non-state enemy is incapable of winning a war, yet it has won the asymmetrical confrontation for years, the declaration of war turns a disadvantage into an advantage.[74] Furthermore, a declaration of war would allow the State of Israel to exert pressure on the other side by withholding the supply of fuel, electricity, water, food, and medical care while fighting as the enemy tries to harm Israel's population and infrastructures. (It should be said that the supplies Israel transfers to the Gaza Strip are already reduced to the bare minimum required on humanitarian grounds. Furthermore, the High Court of Justice has determined that Israel must consider circumstances that pose a risk to human life as affecting the amount of supplies crossing the border.[75] At the same time, the effect of declaring war is different: a declaration of war allows the exertion of real, effective pressure on the enemy's population.)
6. *Focusing and refining the political-to-military-echelon discourse.* A declaration of war would require the refinement of the strategic discourse of the political objective between the echelons[76] that would define the military task and the ways to complete it; the relationship between ends and means.[77] Moreover, if we accept Harkabi's assertion on the use of diplomacy and strategy as two complementary methods of action,[78] then the Israeli government must, vis-à-vis Hamas, create a "complementary opposition"[79] and "balance an aggressive military strategy or severe military blow to Hamas with a political, diplomatic strategy."[80]
7. *Determining the rules of the game*. So far, Israel has allowed Hamas to define the rules of the game, and Hamas has established the nature of the fighting: terrorism and attrition. By means of declaring war, the chances that Israel would seize control of the rules and maximize its advantages would grow. "The side that forces the type of war that favors its strengths can operate effectively to realize its objection, whereas the other side will be less relevant from the outset."[81]

8. *Subordinating the struggle between the parties to the laws of war*. Hamas is aware that Israel and other Western armies are subject to international law and therefore does all it can to exploit what it perceives as its enemy's biggest weakness. Hamas' basic assumption is that Western armies will generally act on the basis of the laws of war, and the organization therefore intentionally engages a policy that falls outside the laws of war. This is, in fact, the foundation for its operational doctrine.[82] A declaration of war subjects the entire conflict to the laws of war where the state enjoys a potential advantage.

While this article has dealt with the advantages of a declaration of war, it has not discussed the inherent disadvantages, including economic ramifications of compensation, for instance.[83]

Conclusion

This article examined whether a declaration of war can be used as a tool for the structural and conceptual transformation of the intractable and protracted conflict between Israel and Hamas. The rounds of violence since 2008 have failed to generate convenient, desirable strategic positioning as these flare-ups can clearly be shown to be spiral fluctuations within the Normal Relations Range of the conflict while they have, at the same time, established an ever-rising trend in the intensity of violence within the range. In fact, Israel is trapped in the reality of an asymmetrical conflict with increasing intensities of violence in which Hamas manages to entrench the power paradox, where Israel's strength becomes its weakness and Hamas's weakness becomes its strength. Changing the reality in which Israel finds itself requires a proactive move that would pose a fundamental surprise to Hamas, one with the power to transform the conflict and change the system.

In our attempt to examine the possible contribution of a declaration of war to the transformation of the conflict's asymmetrical structure in a way that would allow Israel to maximize its advantages over Hamas, we chose to expand the legal definition and relate to the declaration of war as a ritual or ceremony having the capacity to change public awareness and reformulate the rules of the game. The integration of four disciplines − international law, conflict resolution, anthropology and strategic studies − allows the reframing of the asymmetrical conflict, providing a different view of the options the state has for confronting a non-state entity.

Notwithstanding disadvantages and problems inherent in a declaration of war, we have indicated the possibility of reversing reality and adopting a

proactive approach through declaring war in a way that would deny certain advantages from the non-state player in the asymmetrical conflict. We believe that the alternate rationale – based as it is on the assumption that reducing the asymmetrical aspect will help decide the conflict by reducing Hamas's political power and relevance as a governing agent – will help change the structure of the conflict, to use conflict resolution terms, and prepare the ground for another player, such as the PA, to take Hamas' place.

The analysis of the implications in this essay is essentially theoretical, absent an existing test case of an actual declaration of war. Nevertheless, we think the analysis can challenge conventional thought and expand the toolkit at our disposal and create a transformation of the conflict, lay the foundation for rearranging the system, and manage the conflict at a lower level of violence and even end or resolve it altogether.

Notes

1 Giora Eiland, "In War as in War," *Yediot Aharonot*, August 4, 2014.

2 Colin Clark, "Obama to World: We're Back," Breaking Defense, September 12, 2014, http://breakingdefense.com/2014/09/obama-to-world-were-back/?utm_source=Breaking+Defense&utm_campaign=60f34e7ab4-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_4368933672-60f34e7ab4-408029065.

3 According to Maj. Gen. (res.) Israel Tal, this was a war, as is clear from his address at the conference "Operation Protective Edge: Military and Political Lessons" held on September 29, 2014, at the BESA Center at Bar-Ilan University.

4 See, e.g., Richard Behar, "the Media Intifada: Bad Math, Ugly Truths About New York Times In Israel-Hamas War," *Forbes*, August 21, 2014. http://www.forbes.com/sites/richardbehar/2014/08/21/the-media-intifada-bad-math-ugly-truths-about-new-york-times-in-israel-hamas-war; Efraim Karsh, "Hamas War Tactics: Attacks from Civilian Centers," Military - Strategic Information Section, Planning Directory, Israel Defense Force; "Palestinian Suffering Used to Demonize Israel." A lecture at The Begin Sadat Center for Strategic Studies, July 23, 2014.

5 In July 2007, Defense Minister Barak led the Israeli cabinet to declare Hamas a "hostile security entity" in order to try to change the rules of the game. But the declaration carried no legal weight and was certainly not a declaration of war. Furthermore, following that declaration there has been a series of operations in the Gaza Strip during which the rules of the game have not changed in any significant way and are certainly nothing like the rules of the game made possible by virtue of a declaration of war.

6 John P. Lederach, "Conflict Transformation," In *Beyond Intractability*, G. Burgess and H. Burgess, eds. (Boulder, Colorado: Conflict Research

Consortium, University of Colorado, 2003). http://www.beyondintractability.org/essay/transformation/.

7 For more, see Kobi Michael, "Demilitarization of the Gaza Strip: Realistic Goal or Pipe Dream?" in *The Lessons of the Operation Protective Edge*, A. Kurz and S. Brom, eds. (Tel Aviv: Institute for National Security Studies, 2014) http://www.inss.org.il/uploadImages/systemFiles/Demilitarization%20of%20the%20Gaza%20Strip_%20Realistic%20Goal%20or%20Pipe%20Dream_.pdf.

8 Yair Naveh, as cited in Amir Rapaport, "Yair Naveh, in the First Interview about Operation Protective Edge and the IDF's Professional Conduct," *Israel Defense*, January 8, 2015: "I think there was a new political conception, and the army had not adapted its plans and inventories to it, nor its state of mind. What happened in practice was the opposite of how the army had prepared in recent years. In the course of the operation they said, OK, now we're embarking on a war of attrition... If you want to change the army's operating conception that drastically, you first have to carry out orderly debates in the government, decide what the implications and ramifications will be, and prepare accordingly, and not arrive at a 50-day long campaign as if by surprise."

9 Paul Watzlawick, John Weakland and Richard Fisch, *Change: Principles of Problem Formation and Problem Resolution* (New York: W.W. Norton & Co., 1974).

10 Kobi Michael, "Limitations of Strategic Maneuver: The Israeli Case," *Infinity Journal* 1, no. 4 (2011): 12-16.

11 We would like to thank Col. (res.) Pnina Sharvit Baruch, an expert on international law and senior research fellow at the Institute for National Security Studies for her comments and insights on this part of the essay.

12 Jennifer K. Elsea and Richard F. Grimmett, *Declaration of War and Authorizations for the Use of Military Force: Historical Background and Legal Implication* (prepared for members of Committee of Congress USA, March 17, 2011).

13 Yehoshafat Harkabi, *War and Strategy* (Tel Aviv: Ma'arakhot Publishers, 1990).

14 It should be said that there is a difference between a declaration of war and the use of force. In the context of this essay, we examine the transformative aspect of the actual declaration of war rather than the transformative aspect of the use of force. Nonetheless, we must also examine the legal aspect of the act of declaring war because the basis for waging war is legal to begin with. On the basis of this aspect, we wish to add the anthropological aspect and examine the declaration of war as a possible strategy.

15 United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI, http://www.un.org/en/documents/charter/; see also: Robbie Sabel, "Operation Cast Lead and International Law," *Strategic Assessment* 11, no. 4 (2009): 25-28.

16 Beyond the use of force for self- or collective defense, some recognize the right to use force under other circumstances. For more see, Pnina Sharvit Baruch and Brandon Weinstock, "The Use of Chemical Weapons Against the Syrian People: Does It Justify Forceful Intervention?" *Law and National Security: Selected Issues*, P. Sharvit Baruch and A. Kurz, eds. Memorandum 138 (Tel Aviv: Institute for National Security Studies), pp. 11-28, http://www.inss.org.il/uploadImages/systemFiles/memo138110618427.pdf.

17 Laws of War: Opening of Hostilities (Hague III); October 18, 1907, Entered into Force: 26 January 1910. http://avalon.law.yale.edu/20th_century/hague03.asp.

18 Kellogg-Briand Peace Pact (Treaty Providing for the Renunciation of War As an Instrument of National Policy, 46 Stat. 2343 (1929); TS 796; 2 Bevans 732) and the Charter of the United Nations. Treaties prohibit the use of war as part of a national policy. The nations that are party to a treaty bind themselves to resolve conflicts using only peaceful means. Such treaties are the first step to delegitimizing the use of force. Atty. Daniel Reisner goes even further and says that declarations of war are no longer legal by virtue of these charters (in an interview by Ilana Kwartin with Atty. Reisner for her doctoral thesis on December 11, 2011).

19 Elsea and Grimmett, *Declaration of War*, p. 2.

20 For more on the laws of war, see David P. Cavaleri, *The Law of War: Can 20th-Century Standards Apply to the Global War on Terrorism?* (Kansas: Combat Studies Institute Press, 2005); Sabel, "Operation Cast Lead and International Law;" Harkabi, *War and Strategy*; Raphael Biton, "Laws of War as Overall Framework for Regularizing Institutional Killing," *IDF Law Review* 19, IDF Military Advocate General (2007): 245-323.

21 Basic Law: The Government Paragraph 40(c), published in Israel's Statues 2001, No. 1780, March 18, 2001, p. 158 (1999 Bill No. 2756, p. 72).

22 In July 2006, after Hizbollah attacked on Israeli soil, MK Dr. Yossi Beilin submitted a petition to the High Court of Justice against the prime minister and the government of Israel to issue an order nisi to force the government to declare war in Lebanon (High Court of Justice 6204/06, 6235/06, 6274/06 Yossi Beilin et al Versus the Prime Minister et al, court.gov.il). According to Beilin, the Israeli government had acted improperly by not making a decision to go to war based on Basic Law: The Government, Paragraph 40(a) even though it was already, in practice, in a state of war. His petition was rejected, in part because, as determined by Justice Beinish, there had not been a casus belli for a declaration of war as required by law. In rendering her judgment, Justice Beinish stressed that the conditions stipulated by Paragraph 40(a) of Basic Law: The Government had been fully met and an announcement had been given to the Security and Foreign Affairs Committee of the Knesset and then to the Knesset plenum. She also noted that the Emergency Regulations enacted on the basis of the situation dealt

with the possibility of compensating residents and there was no need for a declaration of war to ensure their rights.

23 John L. Austin, *How to do Things with Words: The William James Lectures Delivered at Harvard University in 1955*, J. O. Urmson and M. Sbisà, eds. (Oxford: Clarendon Press, 1962).
24 Yoav Kenny, "Declaration," *Mafte'ah* 1 (2010): 21-33.
25 Ibid.
26 Austin, *How to do Things with Words*.
27 Ibid.
28 Kenny, "Declaration."
29 Arnold van Gennep, as appears in Victor W. Turner, *The Ritual Process: Structure and Anti-structure* (Chicago: Aldine Pub., 1969).
30 Ibid., p. 152.
31 Don Handelman, *Models and Mirrors: Towards an Anthropology of Public Events* (New York: Berghahn Books, 1990), pp. 1-132.
32 Trexler in: Handelman, *Models and Mirrors*, p. 11.
33 Ibid., p. 12.
34 Ibid.
35 The publication of The Journal of Conflict Resolution in 1957 marks the founding of the field.
36 For more on existing approaches in the field of conflict management and resolution, see Robert A. LeVine and Donald T. Campbell, *Ethnocentrism: Theories of Conflict, Ethnic Attitudes and Group Behavior* (New York: Wiley, 1972).
37 Johannes Botes, "Conflict Transformation: A Debate over Semantics or a Crucial Shift in the Theory and Practice of Peace and Conflict Studies?" *The International Journal of Peace Studies* 8, no. 2 (2003). http://www.gmu.edu/programs/icar/ijps/vol8_2/botes.htm.
38 Lederach, "Conflict Transformation."
39 "The old paradigm of conflict resolution is clearly being revised if not in the process of being replaced," Botes, "Conflict Transformation."
40 Oliver Ramsbotham, Tom Woodhouse, and Hugh Miall, "Introduction to Conflict Resolution: Concepts and Definitions," In: *Contemporary Conflict Resolution: The Prevention, Management and Transformation of Deadly Conflicts* (Cambridge: Polity Press, 2005), pp. 3-31.
41 Botes, "Conflict Transformation."
42 Ibid.
43 Lederach, "Conflict Transformation."
44 Louis Kriesberg, "Conflict Transformation," in *Encyclopedia of Violence, Peace and Conflict*, L. Kurz, ed. (New York: Academic Press, 2008), pp. 401-13, p. 407.
45 Botes, "Conflict Transformation."
46 Väyrynen, cited in: J. Botes, "Conflict Transformation."

47 Edward E. Azar, Paul Jureidini, and Ronald McLaurin, "Protracted social conflict; Theory and practice in the Middle East." *Journal of Palestine Studies* (1978): 41-60.

48 Ibid.

49 The tool presents an axis ranging from cooperation to high-intensity violence (the Y axis) and the element of time (the X axis). Azar claims that every conflict can be located on this graph within what he defines as the normal range of the conflict (despite the paradox). According to him, protracted, unresolvable conflicts tend to be volatile and therefore seek to leave the so-called normal range. At the same time, leaving the range means encountering mechanisms (doorkeepers of a sort) whose function is to ensure that the conflict returns to its normal range. This means that a deviation from the range on the Y axis towards escalation arouses in turn regional dangers and perhaps also damage to the interests of international players in the arena, or at least destabilizes the international system and therefore leads to intervention on the part of the international community working to bring the conflict back to the normal range. On the other side of the range, any deviation on the Y axis towards cooperation encounters pressure from the social structure charged with maintaining national solidarity and a shared national identity preventing cooperation.

50 Kobi Michael, "Who Really Dictates What an Existential Threat is," *Journal of Strategic Studies* 32, no. 5 (2009): 687-713.

51 Klaus, J. Gentzel and Torsten Schwinghammer, *Warfare Since the Second World War* (New Jersey: Transaction Publishers, 2000).

52 Hanan Shai, "The Intellectual Challenge in the Struggle Against Human Bombs and Other Inhuman Terrorism", in *Ticking Bombs*, H. Golan and S. Shai, eds. (Tel Aviv: Ma'arakhot, 2006), pp. 167-77.

53 A "strategy of attrition" is defined as a military method of operation with political goals and designed to gradually erode the enemy's fighting power; its objective is to prevent the enemy from winning a military decision. The less powerful side makes every effort to draw the conflict out in time so as to bleed the enemy while delegitimizing the more powerful side and making massive use of psychological warfare via the media to cause cumulative exhaustion and erosion. Moshe Ya'alon, "Between Decision and Victory," *National Security Studies* 2, (2001) http://www.xn--7dbl2a.com/wp-content/uploads/2014/05/%D7%91%D7%99%D7%9F-%D7%94%D7%9B%D7%A8%D7%A2%D7%94-%D7%9C%D7%A0%D7%99%D7%A6%D7%97%D7%95%D7%9F.pdf.

54 Shai, "The Intellectual Challenge."

55 Ramsbotham, Woodhouse and Miall, "Introduction to Conflict Resolution."

56 The test case was extensively discussed in an essay published in a Canadian journal. For more, see Ilana Kwartin and Kobi Michael, "Declaration of War – Between a Ceremony and a Strategy: The Case of Israel and Hamas in the Gaza Strip," *Journal of Politics and Law* 6, No. 3 (2013): 198-208.

57 Azar, Jureidini and McLaurin, "Protracted Social Conflict: Theory and Practice in the Middle East," *Journal of Palestine Studies* 8, no. 1 (1978): pp. 41-60.

58 Although the Gaza Strip is not recognized as a state, it fulfills the four characteristics defining a state noted by the 1931 Montevideo Convention: a defined territory, a population, a government and an independent foreign policy. In addition, the Hamas government in the Gaza Strip has an organized military force as well as police and enforcement mechanisms. Montevideo Convention on the Rights and Duties of States, signed at Montevideo, 26 December 1933, Entered in to Force December 26,1934, LNTS 19; 49 Stat 3097, 165. http://ilsa.org/jessup/jessup15/Montevideo%20Convention.pdf.

59 Montevideo Convention on the Rights and Duties of States, signed at Montevideo, December 26, 1933, Entered in to Force 26 December 1934, http://ilsa.org/jessup/jessup15/Montevideo%20Convention.pdf LNTS 19; 49 Stat 3097, 165.

60 Robert I. Rotberg, "Failed States in a World of Terror," *Foreign Affairs* (2002), http://www.foreignaffairs.com/articles/58046/robert-i-rotberg/failed-states-in-a-world-of-terror.

61 David Reilly, "The Two-Level Game of Failing States: Internal and External Sources of State Failure," *Journal of Conflict Studies* 28 (2008), p. 17.

62 The National Security Strategy of the United States of America, 2002, http://www.whitehouse.gov/administration/eop/nsc/.

63 David Reilly, "The Two-Level Game of Failing States."

64 Daniel Bar-Tal, "The Psychosocial Foundation of Uncontrollable Conflicts: A Conceptualization", in *Living with the Conflict: A Psychosocial Analysis of Israeli Society*, D. Bar-Tal, ed. (Jerusalem: Carmel Publishing, 2007), pp. 24-52.

65 Louis Kriesberg, "Interlocking Conflicts in the Middle East," *Research in Social Movements, Conflicts and Change* 3 (1980): 99-119.

66 Zvi Lanir, *The Fundamental Surprise: Intelligence in Crisis* (Tel Aviv: Kibbutz Me'uhad Publishers, 1983).

67 Gregory J. Sidak, "To Declare War," *Duke Law Journal* 41 (1991): 27-121, http://scholarship.law.duke.edu/dlj/vol41/iss1/2.

68 Ibid.

69 William I. Zartman, *Ripe for Resolution* (New York: Oxford University Press, 1985/1989).

70 Richard Kemp, International Law and Military Operations in Practice. Paper presented at the Joint International conference on Hamas, the Gaza war and Accountability under International Law. Center for public affairs, Jerusalem, July 2009.

71 Ron Tira, "The Struggle over the Nature of War: From Clausewitz to Scipio Africanus and Anwar Sadat and the State Enemy Used to Fighting RMAs," Memorandum 96 (Tel Aviv: Institute for National Security Studies), p. 68.

72 Boaz Zalmanowitz, "The Tactical United States for Fighting Limited Conflicts: Conception, Testing Process and Experiments," *Ma'arakhot* No. 405(2006), pp. 28-33.

73 Erez Wiener, "Fighting Terrorism: Through Direct Contact or by Standoff Fire?" *Ma'arkhot* No. 406, pp. 22-27.

74 "Armed opposition groups are not able to win a direct confrontation with the regular armed forces because they lack firepower, but they can win small local engagements, keep large numbers of regular forces tied up and, perhaps, prevent control by the armed forces of the whole territory." A.P.V. Rogers, "Unequal Combat and the Law of War," *Yearbook of International and Humanitarian Law* 7 (2004), pp. 3-34.

75 See the state's position and its imprimatur by the High Court of Justice in High Court of Justice 9132/07 Al Bassyouni et al Versus the Prime Minister et al; and High Court of Justice 4258/08 Gisha (Gaza Gateway) et al Versus the Minister of Defense.

76 See Michael, "Demilitarization of the Gaza Strip."

77 The Joint Operation Environment (JOE), Distribution Statement A, February 18, 2010, http://fas.org/man/eprint/joe2010.pdf.

78 Harkabi, *War and Strategy*.

79 Kobi Michael, "The Weakness of Statesmanship: Who Really Shapes Israel's Security and Peace Policy and Why" lecture presented at Tel Aviv University conference, 2009.

80 Ibid.

81 Ron Tira, "The Struggle over the Nature of War," p. 68.

82 Richard Kemp, "International Law and Military Operations in Practice." Paper presented at the Joint International conference on Hamas, the Gaza war and Accountability under International Law (Jerusalem: Center for Public Affairs, 2009).

83 The inherent disadvantages of declaring war: 1) irrelevance at the political level as well as the legal one because of its rarity; 2) a declaration of war is liable to lead to internal dissent or widespread panic rather than social cohesion and patriotism of the population; 3) a declaration of war would grant legitimacy to a movement that is defined and recognized as a terrorist organization; 4) the concern that a formal declaration of war is liable to generate an actual war, one of whose consequences would be winning a decision against Hamas and restore Israel to effective control of the Gaza Strip and having to assume responsibility for its population. For more, see Ilana Kwartin and Kobi Michael, "Declaration of War – Between a Ceremony and a Strategy: The Case of Israel and Hamas in the Gaza Strip," *Journal of Politics and Law* 6, no. 3 (2013): 198-208.

The Islamic State's Strategy in Cyberspace

Gabi Siboni, Daniel Cohen, Tal Koren

The success of the Islamic State (henceforth: ISIS) includes the integration of interrelated elements in a way that helps the organization consolidate its control of extensive regions, serve as the current spearhead in the global Jihad effort, and threaten the world with terrorist attacks carried out by its agents holding citizenship in a Western country. These agents are liable to return to their homeland and along with "lone wolves" they are liable to carry out terrorist attacks against targets in the West. The aim of this article is to examine ISIS's model, as it is an organization that has successfully conquered many geographic areas while attracting public attention on an unprecedented global scale. The article will attempt to assess the organization's unique strategy, which combines two key interrelated elements: extensive use of the social media on the one hand and extreme and savage cruelty on the other.

Keywords: Islamic state, ISIS, social media, Iraq, Syria, terrorism

Introduction

In May 2004, an Islamic website published a video clip showing the execution of Nick Berg, a U.S. citizen, in Baghdad. The clip showed Berg in an orange prisoner's uniform (the same worn by prisoners at Guantanamo Prison), beheaded by Abu Musab al-Zarqawi, the leader of al-Qaeda in Iraq. Ten years later, this video assumed horrifying historical significance with the publication of a video clip showing the beheading of American James Foley by agents of ISIS, carrying on the actions of Abu Musab al-Zarqawi.

Dr. Gabi Siboni is a senior research fellow and the head of the INSS Cyber Security Program. Dr. Tal Koren is a research fellow in the Cyber Security Program. Daniel Cohen is a Research Fellow and coordinator of the Cyber Security Program.

The main difference between the two video clips is that the man who beheaded Foley spoke fluent English, and the professionally edited clip was spread virally throughout the entire world. Viewers in Western countries experienced a feeling of horror at the sight of a prisoner being led to the slaughter, not only because the victim seemed like their next-door neighbor, but because the slaughterer also represented the image of a neighbor. ISIS uses the global village of the information era, in which the boundaries between reality and imagination have been blurred using technological means available to everyone, in its call to its supporters in the West to make the hegira (immigration to the Islamic state) or join the jihad - "pack your suitcases or prepare explosive devices."

Psychological warfare in the service of terrorist organizations is not a new phenomenon. Carlos Marighella, one of the fathers of modern revolutionary terrorism, published The Mini-Manual of the Urban Guerilla in the 1960s, in which he referred to a war of "nerves" and psychological warfare. He asserted that governments will always be in a position of inferiority in combating psychological warfare used by a terrorist organization, as a result of the many resources used in counter efforts and censorship. According to Marighella, this investment is doomed to fail. In the digital and new media era, the challenges and threats have changed as a result of the new spheres in which a terrorist organization can operate to promote its political objectives. ISIS operates on a large scale in virtual space by using new media platforms that make censorship difficult. The position of inferiority in defending against this phenomenon is therefore significant, and requires observation and a solution to this threat that makes use of up-to-date tools.

The wave of spontaneous terrorist attacks ("lone wolves") in the U.S., Canada, Australia, Europe, and Israel highlights the emerging symbiotic connection between ISIS's recruitment calls, propaganda, and terrorism against Western civilians and the various communications platforms made possible by virtual space. It incorporates terrorism executed by veterans who fought within ISIS ranks in Syria and Iraq and returned to the west, such as the murder of Israeli couple Mira and Emanuel Riva at the Jewish Museum in Brussels in May 2014 by Mehdi Nemmouche, a French citizen of Algerian origin who returned to Europe after fighting with jihad forces in Syria. These local unorganized terrorist actions, carried out "under the influence of ISIS" and inspired by it, include attacks by shooting and running over pedestrians in Canada, and attempted beheadings in Australia

and the U.S. ISIS employs public relations, recruitment, and propaganda apparatuses in virtual space, including the publication of magazines and high-quality video clips that can be viewed by the international media with restrictions, and sells merchandise with the organization's symbol online. The organization's agents even document and share their comments on social networks. This mode of operation, which includes transparency and ruthlessness, is perfectly suited to the organization's current strategic policy: preparation for global terrorist activity by recruiting foreign agents and establishing new terrorist cells throughout the world. In "The Violent Image: Insurgent Propaganda and the New Revolutionaries," Neville Bolt says that the Islamic State has adopted the idea of "propaganda of the deed," similar to the old tactics used by revolutionary groups, in which violence and communications were merged in order to achieve the maximum effect in delivering a political message. He claims that what is unique about ISIS is its combination of distribution platforms in the media and the new media to display extreme and savage cruelty. This constitutes a new spectrum of "network warfare" involving exploitation of the information revolution. The organization uses reciprocal propaganda, and includes horrific pictures immortalizing terrorism, designed to generate fear and anxiety (such as video clips featuring beheadings), and as means for influencing decision-makers in the West.

The success of ISIS, which has consolidated itself over the past year in Iraq and Syria, and has established organizational infrastructure in North Africa and the Sinai peninsula, includes the integration of interrelated elements in a way that helps the organization consolidate its control of extensive regions and serve as the current spearhead in the global Jihad effort. In addition to posing a threat to the stability of Arab regimes in the Middle East such Saudi Arabia, Jordan, and Lebanon, there is also the threat of terrorist attacks carried out throughout the west by western citizens who have joined ISIS in Syria and Iraq and then returned home, and encouragement of spontaneous terrorist attacks against Western targets. The media and violence are used in tandem to both intimidate nearby enemies and to recruit agents and supporters. These actions, which are being conducted in places geographically proximate to democratic countries (the West), include extensive use of media on the one hand, and extreme and savage cruelty on a previously unseen scale on the other.

These elements are intertwined; aiming at a Western target group and the physical proximity to this target along with the appeal for recruitment

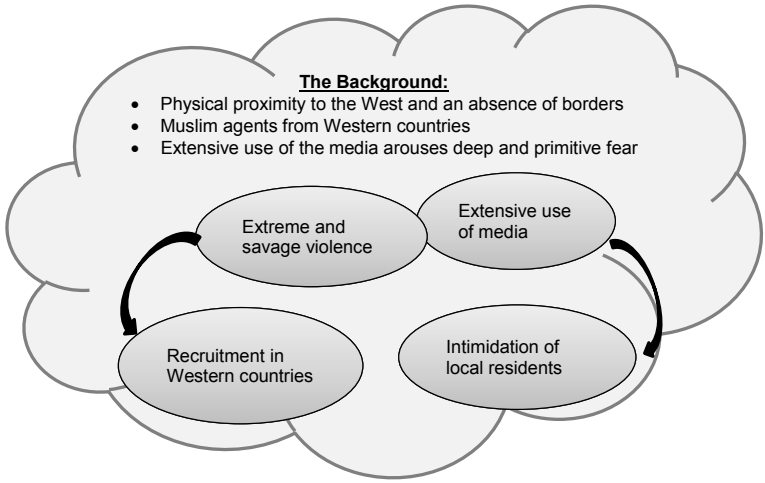


Figure 1. ISIS modus operandi

of supporters from those countries generates a feeling of deep primitive dread among the general public, combined with a strong attraction among the audience of potential supporters (see Figure 1).

This article asserts that ISIS's internet success is due to the connection between its use of extreme ruthless cruelty and the use of cyberspace to spread messages internally and externally for purposes of recruitment and intimidation. The background to this policy is physical proximity to the West and the creation of a deep feeling of dread in Western countries of being inundated with terrorists and supporters of Islamic-motivated violence.

ISIS makes intelligent use of social networks for delivering focused messages to specific target audiences, namely Muslim communities in Western and Asian countries. Up until now, ISIS's media strategy has succeeded in positioning the organization as the main enemy of the West, branding it as the spearhead in the global jihad struggle, winning support among Muslim audiences and jihad organizations.[5]

ISIS Propaganda and Recruitment System

ISIS, like al-Qaeda in its early days, recognizes the fact that it must operate simultaneously on a number of fronts in its war against infidels. The organization therefore regards its media strategy as representing "two thirds of the battle,"[6] and regards the struggle over popular opinion as essential and complementary to its activity.[7] The importance of the media in it various forms as means of gaining influence, support, and sympathy from millions

of Muslims around the world is evident in the organization's activities and the many resources invested for the purpose. The Internet and social networks are the chief means of disseminating its ideology and political messages, as well as means of recruiting foreign volunteers and financing, while being careful to control the flow of information from the battle areas. ISIS uses a number of online platforms,[8] such as the al-Furqan Institute for Public Relations Production,[9] which serves as the official media arm of ISIS and its leaders, and the "al-Athzam Agency for Media Production." This agency has been operating for the past two years, producing ISIS video clips and distributing them on the social networks. Another ISIS media arm is the Islamic State organization website, called the al-Hayat (Life) Media Center, which is aimed mainly at a Western target audience.

The al-Hayat media center contains a great deal of material about ISIS, including speeches and video clips translated into more than 10 languages. The website, which is aimed at the West and a non-Arabic speaking audience, combines content and diverse material with new video clips and subtitles for earlier video clips, in addition to articles, news reports, and translation of jihad material. The website is of high quality, and was probably designed by a team with experience in producing material for a Western audience. ISIS distributes bloody propaganda clips on the Internet, in which the organization showcases the cruel tactics used in its conquests in Syria and Iraq, while boasting the helplessness of its enemies. One of the propaganda films issued in September by the Islamic State, which was professionally edited as a documentary film, is entitled, "Flames of War: The Struggle Has Only Begun."[10] Its purpose is to deliver a clear message against U.S. intervention targeting the organization. The 55-minute film uses carefully designed romantic images, combined with special elements of explosions, battles, wounded American soldiers and those about to be killed, anti-American rhetoric, edited slow-motion segments of executions, and archive segments of Western leaders. The film includes sophisticated illusory elements (size, distorted pictures, enhancement of speakers, a speech lit by torches) resembling the 1934 propaganda film produced in Nazi Germany as a propaganda documentary move by Leni Riefenstahl, "Triumph of the Will."[11]

This movie joins a long series of professionally edited films documenting bombings, terrorist attacks, and assassinations of officials, military, and security forces personnel in Iraq. One example is the popular four-part series entitled "The Clanging of the Swords," the first part of which

was distributed as early as June 2012. The series has gained widespread exposure on platforms such as Twitter and Facebook.[12] A comprehensive analysis of the fourth part of the Clanging of the Swords, aired on May 17, 2014, was published by Nico Prucha and Ali Fisher on the Jihadica website. It describes the level of sophistication demonstrated in the use of the social media and in the use of information distribution technology on various platforms, including cellular telephones (the preferred platform, especially the use of the "Twitter for Android" application), various web technologies, and file sharing websites (justpaste.it, archive.com), with the use of a different size and format, variable quality, and different languages (Arabic, Indonesian, English, German, and Japanese). It is no surprise that the video was released on Saturday as a deliberate strategy to prevent blocking by web companies, as their employees are on their day off. In the first 24 hours after the video was released, there were nearly 60,000 hits (the average viewing time was 17 minutes).[13]

In November 2014, a short film showing the beheading of 22 Syrian prisoners was published. The film was analyzed by the Terrorism Research and Analysis Consortium (TRAC), and the Quilliam Foundation think tank pointed out that the film was professionally produced, including many hours of filming, the use of HD cameras, and professional editing. The analysis concluded that the cost of producing this film was about $200,000.[14] The production of this film reflects the level of savagery as well as the level of sophistication. This film does not document an execution; it is a "reality" film of a mass execution carried out solely by "outside" soldiers recruited to the organization. The "extras" in the film are executed. This method shows the importance attributed by the organization to the use of media, and its profound understanding of the effect that such a film has on viewers; generating a feeling of "romantic" attraction for potential recruits on the one hand, and the creation of a feeling of terror and dread among Western citizens on the other.

In addition to violent material and content, some of its publications are designed to recruit new volunteers from Western and non-Arab countries. The al- Hayat Media Center, for example, published a number of original video clips under the "Mujatweets" headline aimed at showing that life under the Islamic State was peaceful and normal, pointing to a positive aspect that would soften the brutal image of a murderous organization, and in order to attract new recruits.[15] In addition, a series of high-quality articles published as PDF documents, similar to al- Qaeda's "Inspire" online

magazine, can be found on the website aimed at showing and emphasizing the organization's success on the battlefield and portraying prominent soldiers in its ranks. Some of the video clips were designed for the purpose of influencing public opinion by showing scenes of food distribution, medical treatment, and charity. The films have English subtitles, and are designed to convince Western professionals to come and help in the building of the Islamic state. The organization publishes something called the IS Report, which contain articles in English describing the founding of offices for the training of Imams, religious legal rulings, pictures of executions, and victories on the battlefield.[16]

In addition to the ISIS media apparatus distributing the organization's publications on the Internet, ISIS publishes a number of Internet magazines; the most important is the Dabiq periodical.[17] The first issue was published in July 2014 in a large number of languages, and resembled the al-Qaeda "Inspire" magazine in its design. The main emphasis in the first issue, which filled 50 pages and was entitled "The Return of the Calilafah," was to convince its readers of the legitimacy of the caliphate declared by ISIS leader Abu-Bakr al-Baghdadi, and to call upon Muslims from all over the world to come to "their natural country" under its leadership. The other three issues came out in September-October, and included quotations and remarks by senior officials in the organization, hadiths legitimizing slavery as "the spoils of war," information about building the Islamic State, calls for the killing of "Crusaders," justification of executions, etc. Another public relations activity designed to appeal to Muslim communities outside the war zones in Syria and Iraq was the English language "Islamic State News" Internet news magazine, which contained both regular reports about the organization and reflections with an Islamic Salafi-jihadist orientation.[18] ISIS conducts additional forums and official news sites in Arabic on the Internet, such as al- Minbar al- Ilami al- Jihadi[19] (Jihad Forum) and others with diverse propaganda content about ISIS.

For ISIS, the use of social networks is a platform constituting a significant lever enabling the organization to recruit broad support among the young radical Muslim public in their countries of origin and in the West, while delivering focused messages. On the other hand, communications and messages between the global jihad organizations and their supporters, such as al-Qaeda, are usually deployed over the "dark web" that is not accessible to everyone, in mosques, and through distribution of leaflets and designated websites.[20] ISIS has therefore chosen to operate openly on the social media

channels, including YouTube, Twitter, Facebook, and other less well-known social networks that appeal to a Western target audience and in Muslim communities in the West. ISIS is flooding social networks with especially savage and graphic materials of torture, mass execution, beheading, and crucifixion. As noted, however, this is only part of the broader picture. The use of social networks serves a number of purposes, such as psychological warfare and creating a deterrent effect on both a specific target audience in the battle zones and on Western public opinion, creating a presence and image of size in order to give the impression that the organization is larger than it actually is, disseminating ideology, obtaining financing, and calling for volunteers to join jihad, while distributing videos and interviews with Australian, European, and American Muslim citizens.

The organization's use of these networks is highly sophisticated, mainly in transmitting vicious propaganda messages that overshadow the media efforts of competing organizations, such as al-Qaeda and its affiliates. The efforts by Western countries to close accounts affiliated with ISIS and its supporters and censor their content almost never succeed. For example, the Islamic State organization used an application working on the Twitter network called "Dawn of Glad Tidings." Until not long ago, this application, which could be downloaded from the Google Play Store, facilitated automatic posts to the accounts of the organization's supporters. Another method is the use of Hashtag, which is used on social networks (such as Twitter, and Facebook).[21] ISIS uses "Hashtag Hijacking," which is a relatively simple method of implanting popular words, thereby gaining the attention of people looking for certain content. ISIS also uses advanced technologies, as noted in a recent special report published by the ZeroFox Company. This involves taking advantage of computers by inserting malware in order to promote specific campaigns. ISIS also distributes computer games in order to recruit volunteers and supporters, while training and preparing them for the battlefield. One example is a trailer distributed with a computer game called "Jihad Simulator," in which the games simulate abductions, military vehicles' detonation, and shooting at schools.[22] The games facilitate a high level of communications (managing conversations through texts, network cameras, earphones, and microphones), and constitute a convenient way of maintaining an extensive recruitment and training infrastructure.[23]

As part of its well-financed and well-timed media activity, ISIS is initiating major media campaigns designed to encourage joining its ranks, including the issuing of threats against the U.S. and its allies in order to

deter them from intervening in events in Iraq. One such campaign took place on July 19, 2014, and was distributed on various media outlets under the headline "A Billion Muslims Support the Islamic State." The campaign was successful in gaining support when messages were published all over the world following photographs of various sites: the Temple Mount in Jerusalem, the Eiffel Tower in Paris, Big Ben in London, and other landmarks in North America, Europe, and Asia. ISIS also sells souvenirs (shirts, key chains, toy soldiers, and personal items) for propaganda purposes and as an additional source of income. Several months ago, CNN reported that Facebook was taking steps to stop this, so far unsuccessfully.[24]

Psychological Warfare

The savage terrorist theater used by ISIS, the result of a dangerous symbiosis between the terrorist hungry for recognition and exposure, and the media in pursuit of ratings and eager for violent and riveting scripts created by terrorist events,[25] is not a new phenomenon. It is part of a rational strategy aimed at delivering a message that is mainly psychological in nature. In this sense, the use of terrorism by ISIS and similar organizations against British and American civilians is "mainly symbolic and part of propaganda."[26] Given the great cruelty and inhumanity used by the organization and its comprehensive use of cyberspace to distribute this content, ISIS introduces a new method of operation. By its nature, savagery creates an atmosphere of prolonged international interest and awareness. It also shapes its cruel image, sometimes creating the impression of being more powerful than it actually is.

The use of media by ISIS for terrorist purposes is substantially different from previous terrorist attack that won broad international media coverage, such as the 1979-1981 hostage crisis in Iran, the attack on the Twin Towers (2001) and the hostage crisis in a Moscow theater (2002).[27] While the subject of the use of the communications media by terrorists has been extensively researched[28] in an attempt to understand it in the context of symbolic communications theory,[29] ISIS does not regard the victim as "unimportant." The victims (children, journalists, aid workers, and women) are very important, and their selection is designed to target the "soft underbelly" while the organization invests many resources in using kidnapped journalists for propaganda purposes.

A Strategic Change in the Targets of Terrorism

During 2014, ISIS made a number of strategic changes in its targets and modus operandi in the battle zone. In the first stage, the organization focused on creating infrastructure that would enable consolidation of its control of various areas in Syria and Iraq. The organization therefore committed savage terrorist acts against hostile local Sunni populations, symbols of the regime, and religious-based ethnic cleansing. These included the massacre of the Yazidi minority in the Erbil region, the Sinjar Mountains, and the area of the Mosul Dam. This process was accompanied mainly by media threats against the West, and continued until late summer 2014. A document was recently published by the Syrian Observatory for Human Rights documenting the execution of 1,429 people since last June in Syria. Half of the victims were civilians, and half were members of the al-Shaitat Shi'ite tribe in the eastern Deir a-Zor region in eastern Syria.[30]

The second stage began in August 2014, during the formation of the coalition to fight ISIS, the main significance of which was marking the West, particularly the U.S., as a key target for terrorist operations. As part of this change, ISIS brutally beheaded a number of foreigners it had kidnapped (Americans, British, and French), while making manipulative use of the media with the intention of generating horror in the West and the moderate Arab world. At the media level, the well-timed executions by an ISIS soldier of British origin dressed in black, referred to as "Jihadi John" was done under the heading of "A message to America," according to a prepared script, using advanced photography equipment. The messages placed responsibility on the U.S. and Canada, with the threat that any intervention by Western governments would lead to attacks on innocent civilians. According to a November 17 report in *The New York Times*, at least 23 people from 12 countries were kidnapped by ISIS in November 2012-January 2014, some of whom were released for ransom.[31]

In the third stage, beginning in mid-September, ISIS called for attacks on civilians in various Western countries taking part in the coalition formed against the organization. This was expressed in a speech by ISIS leader Abu Mohammad al-Adnani al-Shami under the title: "Indeed, your Lord is ever watchful," in which he called for the killing of "disbelievers" in Western countries.[32] The calls were issued in audio recordings calling for attacks on Western civilians and security forces.[33] The call also appeared in the fourth issue of Dabiq in October. Initial signs of the results of ISIS's call to kill Western civilians can be seen in the thwarted plan to kill civilians

in Australia, the shooting and vehicular attacks in Canada, the axe attack against policemen in Queens in New York, the laying of explosives in Vienna, etc.[34]

The main purpose of the widely publicized beheadings is twofold; on the one hand, it is designed to generate pressure on public opinion, mainly against the governments of the U.K., U.S., and France, and to differentiate ISIS from the other organizations by its ultra-national savagery. On the other hand, it is a source of attraction for potential recruits by appealing to senses of basic Islamic morality in the framework of a return to the fundamentals of early Islam and a rejection of modern Western morality. The beheading of journalist James Foley on August 19 was designed to deliver a threatening message ("a message to America"), while attributing responsibility for his murder to the U.S., stating that any decision or action taken against the Islamic State will lead to attacks on American civilians. The murder of journalist Steven Sotloff on September 2 was also designed to deliver a sharp message to the U.S. ("a second message to America") against the continued aerial attacks by U.S. forces: "as long as your missiles continue to attack our people, our knife will continue to attack your people's throats."[35]

The beheadings are aimed at two target audiences: local and global. The first is not organized; it is part of the desire to wage psychological warfare against opponents from within. This includes propaganda videos, which are usually not well edited. The second and more significant audience, however, consists of the Western world, especially the U.S., the U.K., and Australia, with the purpose of gaining achievements and propaganda, terrorizing public opinion, and recruiting potential operatives. In September-October 2014, ISIS published a number of videos featuring British journalist John Cantlie from the battlefields in Ayn al-Arab (Kobani) designed for propaganda purposes, in which he announces that he will present the "manipulation of the Western media," and that "the West is being dragged into a war it cannot win against thousands of armed men."[36] Syrian Observatory for Human Rights director Rami Abdul Rahman claimed that a large number of soldiers were murdered by beheading, and by placing the head in a public place ISIS wishes to generate terror and dread.[37] It should be noted that the phenomenon of murdering hostages by beheading is not new. Examples can be found, such as the execution of Daniel Pearl in 2002 by the National Movement for the Restoration of Pakistani Sovereignty, beheadings of ethnic Russians and foreigners by Chechen terrorists, and other groups, including Abu Sayyaf in the Philippines, Algerian groups, and the Taliban.

Summary and Insights

In recent months, the Islamic State has exhibited its mastery of social media, which it regards as a legitimate weapon in its war against its opponents in the organization's countries of origin and against the West (the U.S., U.K., and Australia). ISIS uses simple content that makes its objectives and message very clear, with one ultimate purpose: to induce terror through the calculated management of savagery and the complete absence of mercy.[38] The viral campaigns featuring beheading, crucifixions, burnings, and mass executions distributed through the various media are conducted with unprecedented brutality and cruelty. Terrorism is a type of propaganda, and the more cruel elements it includes, the greater its effect and the bigger the impression it leaves. The horrifying graphic description of beheadings, with its focus on a lone defenseless individual, has a greater effect than propaganda achieved through different means, such as car bombs and terrorism, even if the latter's death toll is higher.[39] ISIS is exploiting the inherent potential of global networking and the ability to simultaneously operate various and diverse means of mass influence, based on computer games, the Internet, and social networking.[40] These measures have created a sophisticated and well-timed online propaganda campaign.

ISIS's propaganda machine and the use of the social and communications media fulfill two important functions that are very distinguishable from each other in their purpose, relying on a media platform that did not exist a decade ago. The first is psychological warfare, targeting the morale of the enemy's soldiers. This is not a new strategy. Chinese general and philosopher Sun Tzu (Master Sun) asserted that victory is usually achieved by "selective, instant decapitation of military or societal targets to achieve shock and awe" through the use of cruel and merciless means, such as beheading.[41] The Blitzkrieg in WWII brought a similar concept of intimidating the enemy through psychological warfare by distributing leaflets from the air, messages from very powerful loudspeakers, etc. The second involves gaining support from Western Islamic groups, while unifying the Islamic State's soldiers behind one goal and under one leadership through an appeal for a return to Islamic roots and sanctioning violence by recruits with no need for any further justification.

The combination of cruelty and the use of social networks by ISIS have been very successful so far, and are being used as a very powerful tool in combination with the Islamic State's military arsenal. In an unusual step, the Iraqi government banned the use of social media during the fighting

in June in order to disrupt communications between ISIS members, a ban that continued for 17 days. More than 20 news websites were blocked, including al-Arabiya.[42]

ISIS operates differently than al-Qaeda, which has so far refrained from harming innocent Muslim civilians in order to avoid losing the population's support. Al-Qaeda leader Ayman al-Zawahiri advised that it was better to kill hostages by shooting, and to focus on attacks against the American and Iraqi forces. "You shouldn't be deceived by the praise of some of the zealous young men and their description of you as the sheikh of the slaughterers," he said, adding, "we are in a battle, and more than half of this battle is taking place in the battlefield of the media. And this media battle is a race for the hearts and minds of our people."[43]

In contrast, ISIS has no scruples about means; it also conducts deadly attacks against the local Muslim population, while implementing a murderous ideology in which the Islamic State's vision is realized through provocations, such as pitiless attacks against strategic sites and national infrastructures.[44] ISIS regards the use of rough violence as essential. The use of media, on the other hand, is also essential for effective propaganda.

The success of ISIS in adopting this strategy is reflected in a number of principal characteristics that distinguish its activity from that of other terrorist organizations and constitute criteria for the organization's success: conquering large territories in Syria and Iraq within a relatively short time span, consolidation of its rule, and the establishment of an Islamic Caliphate. The organization, which was founded as a branch of al-Qaeda in Iraq, has spread to eastern Syria and to the north, while exploiting the weakness of the Iraqi regime. It now controls a population of 10-12 million people, one third of Iraq's territory, and one third of Syria, a territory almost equal in size to the entire U.K.

In the context of combating the organization, coalition military operations should be supplemented by action in other spheres. One is locating and disrupting the "money trail" through which the organization successfully operates a widespread financial system to supply its needs. This task requires an intelligence and global economic warfare effort in order to identify and neutralize the parties involved in financing the organization and trading with it. In addition, a supplementary political effort should be made, particularly with Turkey and Qatar, which in their support for radical Islam, ignoring the movement of volunteers to ISIS by way of the border between Turkey and Syria, are maintaining support in both

camps. Finally, there should be an intelligence struggle and operations in cyberspace should be employed as well.

The second element involves reining in the organization's Internet exposure by blocking sites and content. These are used to recruit operatives, generate attacks, raise money, and exert psychological warfare. Legal infrastructure should be created for this purpose, and agreements should be reached with the large Internet companies having commercial interests. The technological ability to take practical measures exists, but without assembling an international task force that will take immediate effective action to remove malware from the Internet, it will be difficult to cope with this phenomenon. This team can also take action to undermine the organization's narrative through counter campaigns on the social networks: "fighting fire with fire."

The third element is designed to deal with spontaneous terrorist attacks in Western countries. Due to the absence of hierarchies in these attacks and the fact that most of the attacks do not require an existing organizational infrastructure in the country in which the attack takes place, it will be necessary to devise suitable tools for dealing with the attacks. One of these tools would be the ability to generate a profile of potential attacks. This profile will be derived from a variety of sources, the chief of which will be an analysis of the characteristics of the Internet activity by the populations likely to produce attackers. It is usually possible to retrospectively find signs indicating a wish to carry out an attack. It is therefore necessary to assemble an international task force that will be able to create the methodology for constructing such a profile and devise the tools to identify potential hazards on the basis of an analysis of regularly collected big data. The main challenge in this approach concerns the assembling of the characteristics in the profile, rather than the technological aspects of the analysis systems. The defense organizations in the Western countries have a common interest, and will therefore be able to cooperate in devising this capability, thereby pooling their capabilities and expediting the implementation of this concept.

The Western countries require a combined effort to cope with the phenomenon before it is too late. ISIS is acting systematically in cyberspace, and creating a successful model for itself. The West, led by the U.S., needs political, legal, economic, operational, and technological action. Only a long-term combination of these aspects can facilitate an effective struggle against the organization and its jihad effort in the West.

Notes

1 As expressed by a soldier in the organization of Canadian origin in a recruitment video clip distributed by ISI in November: https://www.youtube.com/watch?v=Hzg2WMQB3ZA.
2 Carlos Marighella, "Minimanual of the Urban Guerrilla," *Survival* 13, no. 3 (1969): 95-100.
3 Daniel Cohen, "Fighting Islamic State in Cyberspace," *Haaretz*, September 5, 2014, http://www.haaretz.com/opinion/.premium-1.614320.
4 Neville Bolt, *The Violent Image: Insurgent Propaganda and the New Revolutionaries (*London: Hurst & Company, 2012).
5 *ISIS: Portrait of an Organization*, Meir Amit Intelligence and Information Center, document no. 182, November 28, 2014, http://www.terrorism-info.org.il/he/article/20733.
6 "Antiterrorism Seminar Discusses Media Role," *a-Sharq al-Awsat* (November 25, 2005), http://www.aawsat.net/2005/11/article55268813.
7 Angela Gendron, "al-Qaeda : propaganda and media strategy," ITAC Trends in Terrorism Series 2 (2007).
8 For further discussion of the ISIS public relations apparatuses, see the comprehensive analytic study of ISIS, *ISIS: Portrait of an Organization.*
9 The literal translation of al-Furqan is "separation," i.e., separation of truth from lies.
10 Ryan Mauro, "ISIS Releases 'Flames of War' Feature Film to Intimidate West," *The Clarion Project*, September 21, 2014, http://www.clarionproject.org/analysis/isis-releases-flames-war-feature-film-intimidate-west.
11 Brad Conley, "Leni Riefenstahl – Triumph Des Willens [1935] [HD]," February 25, 2014, https://www.youtube.com/watch?v=rclIE-_VZ5g.
12 "Al-Furqan Media Production Presents a New Film of the Islamic State of Iraq and the Levant," Online Jihad Exposed, May 18, 2014, http://www.onlinejihadexposed.com/2014/05/4.html.
13 Nico Prucha, "Is this the Most Successful Release of the Jihadist Video Ever?" *Ideological trends, Iraq, social media*, May 19, 2014, http://www.jihadica.com/is-this-the-most-successful-release-of-a-jihadist-video-ever. And: http://www.jihadica.com/is-this-the-most-successful-release-of-a-jihadist-video-ever-part-2-the-release-of-صليل-الصوارم-الرابع/.
14 See Terrorism Research & Analysis Consortium (TRAC) Press Room, http://www.trackingterrorism.org/content/trac-press-room.
15 "New ISIS Media Company Addresses English, German and French-Speaking Westerners," *MEMRI: Jihad & Terrorism Threat Monitor*, June 23, 2014, http://www.memrijttm.org/new-isis-media-company-targets-english-german-and-french-speaking-westerners.html.
16 For example, see https://azelin.files.wordpress.com/2014/06/islamic-state-of-iraq-and-al-shc481m-22islamic-state-report-122.pdf.

17 According to Muslim tradition, Dabiq is named after the place in northern Syria mentioned in the hadith about the end of days, when a great battle is expected to take place between Islam and the infidels, which the Muslims will win.

18 It is worth noting that in October 2014, al-Qaeda issued *Resurgence*, a new magazine. The newspaper contains 117 pages, including English pages, and focuses on general jihad topics and current content focusing on the organization's activity in the Indian subcontinent. It can be found at http://www.longwarjournal.org/archives/2014/10/al_qaedas_resurgence.php.

19 See al-Platform Media: alplatformmedia.com/vb.

20 "ICT Jihadi Monitoring Group Periodic Review: Bimonthly Report Summary of Information on Jihadist Websites," International Institute for Counter-Terrorism (ICT) at the Interdisciplinary Center at Herzliya (February 2014), http://i-hls.com/wp-content/uploads/2014/06/JWMG122014.pdf.

21 Hashtag is used on social networks to label a given post as part of a given subject by adding a hash mark before the subject, after which content on a specific subject can be found effectively.

22 David Shamah, "Video Games, Twitter Tricks: How ISIS Pulls in the Kids," *Times of Israel*, September 21, 2014, http://www.timesofisrael.com/video-games-twitter-tricks-how-isis-pulls-in-the-kids-2.

23 More discussion about the use of the various media platforms, specifically the use of computer games can be found in an in-depth study published by the Dado Center for Interdisciplinary Military Studies: Daniel Baran and Yossi Levi, "What Does the West Not Understand?" *Between the Poles* 3 (January 2015).

24 Samuel Burke, "Facebook Looks to Block ISIS Clothing Sales," *CNN* (June 25, 2014), http://edition.cnn.com/2014/06/24/world/isis-facebook-merchandise.

25 Gabriel Weinmann and Conrad Winn, *The Theater of Terror: The Mass Media and International Terroris*m (New York: Longman Group, 1993).

26 Stephen L. Carter, "Boston and the Terrible Theater of Terrorism," *Bloomberg*, April 18, 2013, http://www.bloombergview.com/articles/2013-04-18/boston-and-the-terrible-theater-of-terrorism.

27 Gabriel Weinmann, "the Role of the Media in Propagating Terrorism," in *Countering Terrorism: Psychological Strategies*, U. Kumar and M.K. Mandal, eds. (London: SAGE publications, 2012), pp. 182-203.

28 Boaz Ganor, "the News Media in Terrorists' Strategy," *Ma'arachot* 340 (1995), 41; Boaz Ganor, "the counter-terrorism puzzle: a guide for decision makers," Transaction Publishers, 2011.

29 Communications or symbolic interpretation is exchanges of symbols between various objects that alter the advance expectation of events.

30 "In Five Months, ISIS Executed 1,500 People in Syria," *Maariv- NRG Online*, November 17, 2014, http://www.nrg.co.il/online/1/ART2/646/773.html.

31 Karen Yourish, "the Fates of 23 ISIS Hostages in Syria," *New York Times*, November 17, 2014, http://www.nytimes.com/interactive/2014/10/24/world/middleeast/the-fate-of-23-hostages-in-syria.html?_r=0.

32 Robert Spencer, "Islamic State: 'We Will Conquer Your Rome, Break Your Crosses, and Enslave Your Women, by the Permission of Allah'," *Jihad Watch*, September 21, 2014, http://www.jihadwatch.org/2014/09/islamic-state-we-will-conquer-your-rome-break-your-crosses-and-enslave-your-women-by-the-permission-of-allah.

33 The recording can be heard through the following link: http://ent.siteintelgroup.com/Statements/is-spokesman-had-called-for-lone-wolf-attacks-in-australia-in-september-2014-speech.html.

34 For example, Perry Chiaramonte, "Citizen Jihadists: ISIS Uses 'Lone wolves' to Mount Cheap, Effective Attacks on US Soil," *FOX News*, October 25, 2014, http://www.foxnews.com/world/2014/10/25/citizen-jihadists-isis-uses-lone-wolves-to-mount-cheap-effective-attacks-on-us/.

35 (GRAPHIC VIDEO) Islamic State Beheads American Journalist Steven Sotloff, http://leaksource.info/2014/09/02/graphic-video-islamic-state-beheads-american-journalist-steven-sotloff/.

36 "ISIS Publishes Video of Kidnapped Journalist 'I'm Going to Show You the Truth,'" *Ynet*, August 18, 2014, http://www.ynet.co.il/articles/0,7340,L-4572689,00.html.

37 The exact quote: "In order to strike terror into civilians and into any group that might decide to fight it," taken from: "Over 1,400 People Executed in Syria by Isis in 5 Months: Monitor," November 19, 2014, http://khabarsoutheastasia.com/en_GB/articles/apwi/articles/newsbriefs/2014/11/19/newsbrief-01.

38 Alastair Cooke, "The ISIS's 'Management of Savagery' in Iraq," *World Post,* updated August 30, 2014, http://www.huffingtonpost.com/alastair-crooke/iraq-isis-alqaeda_b_5542575.html.

39 Shashank Joshi, "Where Does the Islamic State's Fetish with Beheading People Come From?" *Telegraph*, September 14, 2014, http://www.telegraph.co.uk/news/worldnews/middleeast/syria/11071276/Where-does-the-Islamic-States-fetish-with-beheading-people-come-from.html.

40 Baran and Levi, "What Does the West Not Understand?"

41 Harlan K. Ullman and James P. Wade, "Shock and Awe, Architecting Rapid Dominance," Chapter 2, NDU Press Book (December 1996), http://www.globalsecurity.org/military/library/report/1996/shock-n-awe_ch2.html.

42 Matt Smith, "Iraq Lifts Social Media Ban, Some Websites Still Blocked," *al-Arabiya News*, July 1, 2014, http://english.alarabiya.net/en/media/2014/07/01/Iraq-lifts-social-media-ban-some-websites-still-blocked.html.

43 Craig Whitlock, "Keeping al-Qaeda in His Grip," *Washington Post*, April 16, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/04/15/AR2006041501130.html.

44 Abu Bakr Naji, *The Management of Savagery: the Most Critical Stage through which the Umma Will Pass*. Translated by William McCants (Cambridge: The John M. Olin Institute for Strategic Studies at Harvard University, 2006).

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