Consistency of Civil-Military Relations in the Israel Defense Forces
The Defensive Mode in Cyber

Glen Segell, PhD

Abstract: The Israel Defense Forces (IDF) has four battle threats, where cyber is equitable to conventional (state), subconventional (nonstate), and nonconventional. An escalation in one could lead to an overall escalation in all. In the political areas and, by extension, in civil-military relations (CMR), the IDF has a defensive mode as routine, while an offensive mode is manifest rarely in emergencies and war. The IDF is engaged in a total war in a defensive mode yet a limited war in the offensive mode as Israel's adversaries do not share the same policies with regular cyber and terror attacks against civilian, government, and military targets. There is consistency in all four threats. Fencing, active defense, and preventive and preemptive strikes dominate.

Keywords: Israel Defense Forces, IDF, civil-military relations, CMR, cyber, limited war, total war, deterrence, defensive mode

Introduction

In 2014, the then-chief of the General Staff of the Israel Defense Forces (IDF *tsahal* צה"ל), Lieutenant General Gadi Eizenkot, created the first cyber branch within the IDF to consolidate all of Israel's cyber capabilities into a single entity.[1] In 2015, Eizenkot authorized the first-ever release of the *Israel Defense Forces Strategy Document* (hereafter *IDF Strategy Document*) to the pub-

Dr. Glen Segell is a research fellow at the Ezri Center for Iran and Gulf States Research, University of Haifa, Israel, and in the Department of Political Studies and Governance, University of the Free State, South Africa. He specializes in intelligence studies, civil-military relations, and strategic communications. He holds the rank of brigadier general (Reserves), where he also consults as an expert for the North Atlantic Treaty Organization (NATO). He was in active intelligence and offense operations in Iraq, Kuwait, Sudan, and Libya.

lic realm. It informed the public of the IDFs' efforts in planning, preparation, training, and defense to meet all threats including cyber, where an escalation in one battle space could also be, or lead to, an escalation in others, especially if the adversaries were the same.[2] The IDF spokesperson stated that the purpose of the document was to "provide a systemic analysis and definition of the context in which the concept was developed."[3] In 2018, Eizenkot for the first time located cyber as the fourth realm of battle threats and spaces alongside other weapons and spaces of operation, namely land, sea, and air. The three other battle threats are conventional (state), subconventional (nonstate), and nonconventional.[4]

This article examines the consistency of civil-military relations (CMR) for all four battle threats and spaces. Such consistency is evident in a combined and joint conformity in the decision making of the civilian government and the application or implementation of these decisions by the military. A policy decision by the civilian government and the military implementation of the decision on the tactical level action for one battle threat and space is the same for the others. This shows that the conformity is in the act of matching attitudes, beliefs, and behaviors to norms, politics and like-mindedness. The norms are implicit, specific rules shared by the civilian government and the military on who is the adversary and how to defeat them that guide their interactions with each other in civil-military relations. This consistency of behaving or performing in the same manner is for all four battle threats and spaces.

The consistency is evident, for example, if an attack and an attacker are a combination of intent and means in any space, then there is no reason why cyber should be treated any differently in the decision making of civil-military relations to that of an attack in the subconventional (nonstate) space, especially if it is the same attacker, for example Hamas. For Israel, it is the same attackers/adversaries in all four spaces and for all four battle threats; in 2021, these include Iran and Iranian proxies such as Hezbollah and Hamas as well as other smaller but more extremist Islamic groups such as the Islamic Jihad Movement in Palestine. In CMR, it is the same democratically elected civilian leaders that have the parliamentary (Israel Knesset) legitimacy and authority to determine the political direction for the IDF to engage in combat against them. Following the process and procedures of CMR, it is the IDF and its soldiers that are tasked with implementing the political decisions. The generals and the soldiers are the professionals who can decide on the best means to do so, commonly known as strategy and tactics.

Commentators in Israeli think tanks speculated that when Eizenkot made the document public for the first time in 2015, it was the fourth of this type of document written since 2002. The goal of the documents had CMR in mind to increase the transparency between the IDF, the political echelon, and the public as a response to the absence of official national security documents.[5] Transpar-

ency and openness was indeed a unique act, yet the content was not a surprise. The content served only to confirm in writing what was already known about the consistency in CMR; in CMR, and by extension in Israeli strategy, both the democratically elected civilian government and the military have a central core of generally shared organizing ideas concerning its national security. That is that the broad purpose of Israel's strategy is the deterrence of aggression and the clear-cut defeat of the enemy if deterrence fails.[6]

In Israeli CMR, there is no evidence that the civilian government seeks military versus political solutions. Rather, it is standard for them to consult with the defense and security organizations to calculate the consequences and ramifications of any decision when engaging adversaries, including considering casualties, and in doing so the most frequent decision is to prefer defense and diplomacy over war. By extension in CMR, the IDF is subservient to the elected civilian leadership of when to go to combat and against whom but decides how to implement the war. The security concept of this has three basic pillars: deterrence, early warning, and decisive defeat (*hachra'a* הכרעה) as the basis for the thinking of being in a strategically defensive mode as routine for all four battle threats and spaces.

Routine is a sequence of actions regularly followed. It is the regular procedure. It is the most accurate translation possible of the Hebrew word (*shigra* שגרה) used in the IDF regularly to indicate no changes for daily military activities in any unit. Such a routine is differentiated from an action or procedure that is undertaken or performed for a special reason. While the defensive mode is routine on a daily basis, an offensive mode is manifest only rarely for a special reason such as in emergencies and in escalations to counterinsurgency battles and war.[7]

With the progression of technology, active defense has been added to this routine military toolbox of defense and deterrence. Active defense serves to support the offense when required, and this in effect enables IDF thinking to be operationally offensive as part of the defensive, or in other words to act in preventive or preemptive combat. One area where active defense thinking prevails is when answering, "What is to be defended?" or when discerning between defense and protection. Defense may be repulsing enemy forces attempting to enter territory, while protection is evident, for example in fencing, in antimissile/rocket systems such as the Iron Dome system, and in cyber.[8]

In operationally offensive cyber, using active defense could be manifest as "defensive cyberspace operations—response action" (DCO-RA). These are those "deliberate, authorized defensive actions which are taken to defeat ongoing or imminent threats."[9] Here then is a case of the consistency in CMR for the four battle threats and spaces. It is also where the security concept in practice links kinetic (conventional) with cyber in combat. This was evident, for exam-

ple, in 2007 when the IDF employed cyber capabilities and electronic attacks to suppress an enemy air defense network so that Israeli Air Force jets could destroy a suspected nuclear facility in Syria.[10]

The defensive mode is evident also in daily routine as few of the male and female conscripts in the IDF see combat during their national service. The majority of the 10 percent of conscripts who are in frontline combat are in the land forces where a majority spend most of their service in training and on border patrols. The rest are in support roles. Similarly, those in the navy spend most of their time in training and patrols with few interdictions or skirmishes.[11] Yet for those in air there is more combat; for example, in 2020, there were more than 500 bombings of munitions and convoy targets in Syria. Those serving in cyber units, although not in physical combat, are more likely to defend against cyberattacks, though they might also be engaged regularly in DCO-RA support.[12]

This article will continue to set the case to test the hypothesis of the consistency in CMR for all four battle spaces and threats, with the IDF engaged in a total war in a defensive mode as routine, yet a limited war in the offensive mode in emergencies, escalations to counterinsurgency, and war. This will be examined in three sections, each with subsections. The first section provides definitions and outlines the concepts examined, including lessons for cyber from conventional and subconventional battle threats, limited and total wars, and limited cyber battles. The second section provides examples that examine the hypothesis, including planning and preparation, authority and jurisdiction, fencing the battle terrain, and mapping the battle terrain. The third section examines how cyber evolved to the significance of being a battle threat and space equitable to the others based on three time frames: the first period from 1993–2003, the second period from 2004–13, and the final period from 2014 to the present.

The Consistency of the Defensive Mode across the Four Battle Threats

This section provides definitions and outlines the concepts of Israel's defense doctrine that views war as the "no choice option," which carries a heavy social and economic price tag. Therefore, Israeli doctrine relies heavily on the defensive mode that includes the projection of deterrence.[13] There are three subsections: lessons for cyber from conventional and subconventional battle threats, limited and total wars, and limited cyber battles.

Lessons for Cyber from Conventional and Subconventional Battle Threats

The military duration of Israel's three interstate conventional wars before the cyber age were the Suez Crises (1956) for one week and two days, the Six Day War (1967) for six days, and the Yom Kippur War (1973) for two weeks and

five days. Such decisive conventional victories may well have deterred more interstate conventional wars as the IDF not only defeated the combined military forces of state adversaries on three geographical fronts simultaneously in 1967 and 1973, but it also conquered territory to more than double its own size in 1967.[14]

Lessons from the conventional battlespace that have been adopted into the cyber, subconventional, and nonconventional battlespaces are based on the distinction between three national situation levels in the context of which deterrence must be achieved and the defensive mode implemented. These are routine, emergency, and war. War is to be avoided as a single defeat may destroy the state. The defensive mode is routine. The daily routine is not to engage in combat. Compellence and preemption of offensive capabilities of the enemy in an emergency is an instrument for inducing deterrence (pre-terrence). To implement the defensive mode for these national situation levels in cyberspace, the IDF has adopted a comprehensive cybersecurity policy approach with a specific focus on developing cyber robustness, cyber resilience, and capacity.[15]

There is consistency for how this is achieved; cyber uses many of the same concepts as conventional tactics. This is with state-of-the-art technology and flexibility of equipment with an integration in the thinking, tactics, and strategy of the kinetic weapon (conventional) with cyber. Cyber equipment as with conventional equipment is procured, which enables switching between offensive and defensive modes. The cyber equipment, both hardware and software, is the same for the offensive and the defensive modes, and therefore training for the defensive also has the capacity for the offensive. Experience from the conventional battlespace, for example, is the Israeli Air Force that has invested in flexible weapon systems and multi-role combat aircraft capable of carrying out both offensive action—bombing enemy targets—and defensive missions—intercepting enemy aircraft in Israel's airspace.[16]

While the IDF has been less effective operationally in subconventional spaces than the interstate conventional wars, the experience and lessons learned from both have also been applied and implemented in cyber. For example, the subconventional battle threat is an asymmetrical confrontation where the outcome appears to demand a political solution rather than a military option. Whereas a single Israeli victory evident in the conventional wars could achieve deterrence against states, such single successes cannot settle the subconventional conflict against radicals and terrorist organizations.

In the subconventional conflict, counterinsurgency military campaigns, such as those in Gaza and Lebanon, have been limited in scope and duration as needed. Such counterinsurgency deployment in Southern Lebanon from 1982 to 2000 did not resolve terrorism coming from there. Public opinion and with

it political action are against deploying IDF ground forces deep inside adversary territory for a sustained duration, as that would result in heavy casualties.[17]

Indicative of consistency, these experiences and lessons learned are extended into cyber. With the subconventional as it relates to cyber, it is accepted that any military option will not end the hostilities. Here a cyberattack is also a military attack as it is a weapon that can cause damage, and the response can similarly inflict damage and casualties. The routine then is the defensive mode and not offensive, not even cyber. As with the conventional and subconventional battle threats, the IDF approach to the cyber battle threat is not to engage in protracted conflict as routine. The projection of nonnuclear (conventional) deterrence is conveyed in cyber, as in the conventional and subconventional battle spaces, as the form of any attack will have a similar response.[18]

This is predicated on the role of compellence and preemption of offensive capabilities of the enemy as an instrument for inducing deterrence (preterrence). As with the subconventional, the IDF undertakes cyber offensives of specific targets for specific or limited purposes. The objective is a measure of active defense—preemptive or preventive strikes. For example, they could be part of DCO-RA operations, but as in the physical domains, caution is taken to assess the effects of countermeasures as they are limited and could typically only degrade, not defeat, an adversary's activities.[19]

Limited and Total Wars

The consistency in CMR with the defensive mode as routine starts with the political objective. The political objective determines the aim of combat or why the war is being fought. This provides an understanding of how the war is to be waged—the military implementation. Conceptually, this is evident in the distinction between two forms of war—limited and total—both politically and militarily. As defined, a *limited war* militarily is one where the belligerents do not expend all of the resources at their disposal. These could be human, industrial, agricultural, military, natural, technological, or otherwise and have specific targets and goals and time frames.[20]

In deciding on a limit for war, an assessment and evaluation of capability and capacity and the adversary themselves determines both politically and militarily the value of expending resources. Politically, Israel's subconventional adversaries are on international terrorist lists. Hamas has been on the United States Foreign Terrorist Organizations list since 1997.[21] Also, Hezbollah and Hamas are both on the European Union's terrorist list.[22] These cannot be targeted easily for they are barely distinguishable from the civilian populations they coexist with. Militarily then, even if the IDF used all the resources in Israel, there is no evidence to suggest that this would bring an end to hostilities. With

this in mind, the IDF is in defensive mode as routine with offensive combat limited.

Conversely, Israel's subconventional adversaries do not function the same. For example, Hamas in Gaza and Hezbollah in Lebanon do not have an electorate to answer to, they do not recognize the right of the State of Israel to exist, and will not enter into any negotiations to end hostilities and conflict. Their regular use of violence and terror with all available resources at civil and military targets alike could well be considered as engaging in a total war against Israel.[23]

As defined militarily and politically, *total war* is where nothing and no one is exempt and includes any and all civilian-associated resources and infrastructure as legitimate military targets, mobilization of all of the resources of society to fight the war, and priority is given to warfare over noncombatant needs.[24] Both Hamas and Hezbollah meet this definition, attacking Israeli civilians, government, and military targets.

Furthermore, Iran is evident in all four battle spaces and threats. The potential conveyed in the *IDF Strategy Document* was "for an escalation in one battle space that could also be, or lead to, an escalation in others, especially if the adversaries were the same."[25] A scenario could be that Hamas and Hezbollah, being the proxy of Iran, and together with Iran, would act in unison and escalate in response to an IDF offensive in one of the battle spaces. As a routine then the IDF is in "defensive mode in cyber and rests on limited cyber offensive activities where cyber is locating equitably along other spaces of operation and threats."[26]

Limited Cyber Battle

The two main features distinguishing limited and total war are the use of resources and targets that could also determine the duration and intensity of the combat. In the CMR in all four battle spaces and threats, the IDF is limited by the political echelons in targeting both in its geographical and demographic jurisdictions.[27] In limiting these, the IDFs' roles and mission are defined and differentiate military with security. As the military, the IDF has a limited cyber battle in a defensive mode compared to that of the more comprehensive or total cyber battle of the security organizations that are in a more proactive offensive mode investigating, arresting, and prosecuting cyber criminals. A brief look at these differences explains this.

The geographical parameter for the IDF is the external defense of the State of Israel—that is, its borders. The IDF may be deployed within the state's borders in civil support (e.g., education) and in emergencies (e.g., earthquakes and medical support). If there is doubt, then the line is drawn when defining the target, namely the specific missions and roles of the IDF. The citizens of the state and other civilians are not normally a military target using any means, including cyber, both within the state or externally in other states.[28]

A distinction on the specific missions and roles of the IDF was evident when the then-Chief of the General Staff Lieutenant General Gadi Eizenkot did not mention other weaponized forms of warfare: information, psychological, and political warfare when he located cyber as the fourth of battle threats along other weapons and spaces of operation, namely land, sea, and air.[29] This could be explained, as for Eizenkot and his predecessors security is different to defense/military, and moreover the IDF does not target civilians, only military combatants.[30]

The various other actors in the Israeli security structures, such as the police, the Border Police (MAGAV מג"ב), and the Israeli Security Agency (ISA/Shin Bet/*shabak* שב"כ)—and not the IDF—are deployed within the state's borders investigating, targeting, arresting, and prosecuting civilians including the subconventional (terrorists) and cyber spaces and threats. Throughout Israel's history, it was these agencies and not the IDF that were the main operatives for the task of the psychological or information operations dealing with Palestinians within Israel's borders and governance area, including the West Bank, Gaza, and East Jerusalem.[31]

The security organizations and not the IDF handled Israel's propaganda and outreach targeting Palestinians during the 1956 and 1967 wars and psychological operations during the period of counterinfiltration operations against the Palestine Liberation Organization's (PLO) attempted infiltrations of terrorists from Jordan and Lebanon during the 1960s, 1970s, and 1980s, before adequate fencing was constructed to prevent these cross-border infiltrations.[32] The security organizations also handled the "winning the hearts and minds" psychological operations in the Second Intifada (2000–5).[33]

Another case is the anti-Israel cyber activists/hactivists, and these could also be mainly civilians and therefore outside of the targeting jurisdiction of the IDF. Such activism/hactivism is in the largely global and unregulated internet, or the cyber underworld, that provokes a response by pro-Israel cyber activists and the security establishment.[34]

Similarly, there is not exact data and information for an accurate analysis on the full extent of IDF units that operate in close cooperation and coordination with the security organizations, as the same radicals and terrorist organizations operate both from outside and within Israel. There are, however, known to be information, psychological, and political warfare units in the IDF, especially elements of IDF Intelligence Unit 8200.[35]

The Determination and Implementation of Civil-Military Relations

The laws of the State of Israel grant the democratically elected civilian government the ability to determine the political decisions relating to adversaries,

while the IDF decides the military implementation. This process takes the form of a constant debate and discussion by the leaders in the civilian government and the leaders in the defense and security organizations, where this debate is the definition of civil-military relations (CMR). In the debate, the IDF is deemed the professional entity with the expertise and so advises the civilian government's decisions on what is viable militarily. It is the civilian government who weighs the options and makes the decision as to whether to use a military option.[36]

As cyber is one of the four battle spaces and threats along with conventional (state), subconventional (nonstate), and nonconventional, then it is fair to say that there is a cyber battle terrain and that cyber is a true type of weapon. In examining the IDFs' role in CMR to implement any decision taken by the civilian government, and given the consistency in CMR for all four in the defensive mode as routine, this section uses case studies to examine the specific cyber weapon with examples in four subsections: planning and preparation, authority and jurisdiction, fencing the battle terrain, and mapping the battle terrain.

Planning and Preparation

The IDF planning and preparation for routine, emergency, or war on any battle terrain have been with specific threats against Israel in mind. In 2021, these are from Iran and its nonstate proxies—Hamas in Gaza and Hezbollah in Lebanon. One aspect of such planning and preparation is based on scenarios. One scenario is the potential escalation from one battle space to an overall escalation in all four battle spaces, thereby making planning for all four battle threats extensions of each other.[37]

A specific scenario is the result of a cyberattack from any one of these adversaries, for example, hacking to falsify sensor signals in an electricity power station that would lead to physical damage of the power station and electricity outages. Citizens and the economy may face significant damage from this.[38]

Protecting and thwarting such an attack would be the responsibility of the electricity company, private expert cyber contractors, and the security organizations while the IDF would be tasked to collaborate in the provision of advice and intelligence. It is the specific role and mission of the IDF, if such an attack did take place by a combatant adversary such as Iran, Hamas, and Hezbollah, to implement a response. The IDF also needs to respond in a way that would not lead to an escalation and would also deter any further attacks. The severity and nature of such an attack and the responses required shows why cyber bears many similarities to other types of weapons and military attacks. A cyberattack using a cyber weapon "is an attempt to expose, alter, disable, destroy, steal, or gain access."[39]

Considering such a scenario, and given the potential for an escalation across

all four battle spaces and threats with the same adversaries and the consistency in having to deter through a strong defensive posture, explains why IDF cyber capacity—both equipment and training—has been developed as part of its arsenal integrating cyber with other tactics, strategy, and weapons.[40]

Experience and lessons from the other battle spaces and threats have been applied to cyber. For example, conceptually, cyberspace is a space as are air and sea spaces. The IDFs' task is to plan and to prepare to control any space, especially where there may be a threat. The similarities also extend to procurement and training. Aircraft and ships may be flexible platforms for many various systems, both offensive and defensive.[41]

Computers as the hardware are also flexible platforms for different types of software. Basic training on information systems, infrastructures, computer networks, or even personal computer devices for the offensive mode is no different from that of the defensive. Specialist training is required and provided for the specific weapon system; in cyber, it is the software.[42]

Experience and lessons in the planning, preparing, procurement, and training from the navy and air force can be conceptually applied to cyber. As the four battle spaces and threats are on a continuum, there then could be symbiotic kinetic (conventional) and cyber efforts to achieve the same objectives of deterrence and defense.

An example of an IDF response to a Hamas cyberattack was not cyber but was an air strike on the building housing Hamas cyber attackers in 2019.[43] Other examples are DCO-RA operations where IDF cyber capabilities and electronic attacks suppressed Syrian air defense networks to enable Israeli Air Force jets to strike more than 500 targets in 2020, mainly arms transfers and supply routes, possibly from Iran to Hezbollah.[44]

Authority and Jurisdiction

The IDF in all four battle spaces as a routine is in the defensive mode, yet it has also planned and prepared to be operationally offensive. That stems from the basic universal principles that any state is entitled to defend its existence, including using armed force.[45]

There are at the same time important instances and circumstances that limits the propensity in CMR to grant the IDF the general authority and jurisdiction to implement preventive and preemptive strikes for immediate military response if attacked and to attack targets of opportunity. A prime reason is caution. An intelligence or other failure could lead to the wrong target being attacked with the consequence being an escalation that might extend beyond cyber and into a full conventional war. For example, the attacker could be an individual terrorist but operating from another country that spoofs their identity to another person in another country.[46]

The caution on escalation is explained by demography, geography, economics, and casualties. Israel has no geographical strategic depth; it cannot absorb an armed attack by adversarial conventional forces. Mobilization of reserves in an emergency for more than a month or two, and with physical damage to industry and commerce, would be at the expense of the economy. Probably the most significant factor that influences political decision makers is the potential for many casualties, both military and civilian. Most of the population lives in a narrow stretch of dense urban dwellings in the Jerusalem-Tel Aviv corridor and could be annihilated in any mass aerial attack.[47] Moreover, the IDF is a people's army. All the soldiers are citizens and all the citizens are soldiers. Casualties are the fathers or the sons in any family, or indeed daughters as women also have compulsory service. And citizens have grumbled and protested that the government and the IDF are not doing enough.[48]

Such existential considerations offer the essential explanation for the consistency in CMR through all four battle spaces and threats to limit the offensive mode. They offer justification to Israel's defense doctrine where any act that might escalate to war is a no-choice option, which carries a heavy social and economic price tag. Given the caution for escalation, cyber as a weapon and as a battle terrain is located firmly in this same doctrine that relies heavily on the projection of deterrence with the defensive mode as routine.[49]

Fencing the Battle Terrain

With the political option preferred over the military option in CMR, see the last interstate war in 1973 and peace treaties with Israel's southern neighbor Egypt (1977) and eastern neighbor Jordan (1994). The residual defense status quo of politically unresolved issues, for example the Palestinian question, sees consistent low-intensity terror and attacks from terror groups in the subconventional and cyber spaces. There are occasional escalations to counterinsurgency with limited campaigns, for example, in Gaza and Lebanon. The status quo is not one where there is any disagreement between the political and the military. The asymmetrical nature of these campaigns and their religious, ethnic, and territorial issues does not lead easily to a military option. Even extended operations to buffer from subconventional attacks (rockets) and working with proxy forces from 1982 to 2000 in Lebanon with the South Lebanese Army have not resolved the status quo.

This political status quo with an inability to have a decisive military solution leads to a consistency in CMR for the defensive mode for all four battle spaces and threats. The defensive mode is not just passive and waiting to repel an attack. The defensive mode has active characteristics and options that are evident when posing the question, "What is to be defended?" This discerns between active and passive defense and protection. Active defense may be DCO-

RA that when implemented could link kinetic (conventional) with cyber. For example, in 2007, the IDF employed cyber capabilities and electronic attacks to suppress an enemy air defense network so that Israeli Air Force jets could destroy a suspected nuclear facility in Syria.[50]

Protection is an example of the IDF defending the borders of the State of Israel using fencing. Throughout the 1950s and 1960s in the subconventional space and threat, Palestinian *Fedayeen* crossed into Israel from Egypt, Jordan, Lebanon, and Syria, attacking civilian and military targets. Progressively over decades, border fences were erected around local agriculture settlements and then cities and finally around the whole border of Israel. Israel aimed to have a closed land, sea, and air space.[51]

New and more formidable fences were progressively erected along the northern Lebanese border to prevent PLO incursions in the 1970s and 1980s.[52] Then a more sophisticated seven-mile long land berm (earth barrier) fence was constructed on the same border to defend against the Iranian-backed Hezbollah that replaced the PLO.[53] A wall has been constructed in the West Bank after the Second Intifada (civilian uprising that saw 171 suicide bombings).[54] Since 2005, fences have been erected to prevent Hamas incursions from Gaza on the southern border and then replaced with more sophisticated ones.[55]

Such fencing has progressively included cyber elements. In the fences and the wall, technology has played a role. In the 1960s, there were electric tripwire border fences, in the 1970s the fences were watched with closed-circuit television surveillance (CCTV), and by the 1990s drone surveillance. Now software programs reduce the need to have a human operator man the audio, visual, and infrared surveillance on a 24/7 basis. The automated systems can monitor Israel's border fencing and instantly alert forces on the ground, air, and sea of an incursion or a pending incursion. Or there could even be remotely controlled responses such as missiles from drones.[56]

As with territorial space, cyber is also a space that needs to be defended and protected. Computers and software are the weapons wielded by human hands and networked computing is the battle terrain space. The experience from the border fencing defensive concept of protecting Israel's territorial borders has reduced the frequency and intensity of attacks. It would not be innovative to suggest that cyber fencing is solely an IDF tactic or measure as it is used worldwide. And it is effective to a large extent.

The basic notion of cyber fencing is to have essential government and military computer infrastructure on a separate physical network from publicly accessible networks. This is not perfect, as with physical fencing's weaknesses there are also weaknesses in cyber fencing. For instance, wireless, satellite, and Wi-Fi communication with forces in the field could be intercepted and false data inserted. There are active measures such as encryption of data that could be taken

to prevent this. Another weakness is when networks and software upgrades are provided from commercial providers that might have malware or viruses.[57]

Mapping the Battle Terrain

While fencing (protection) may reduce the frequency and intensity that the IDF engages in subconventional and cyber combat and also prevents civilian casualties and damage, it can serve to stress that neither the political nor military option are viable to negate and neutralize Israel's adversaries. The defensive mode is preferred, though in an emergency, threat reduction by targeting (active defensive) is another means in the military toolbox.

To implement threat reduction using targeting, the IDF is tasked with mapping the battle terrain. Once the adversary has been identified and located then they can be targeted. In the subconventional (conventional/kinetic) battlefield, the IDF has implemented pinpoint air strikes on adversaries' rocket launch sites, weapons arsenals, and terrorist camps and the occasional targeted assassination.

An example is when, on 12 November 2019 at 0400, Baha Abu al-Ata, a militant leader of the radical Palestine Islamic Jihad in Gaza, was targeted and assassinated by two missiles launched from an Israeli Air Force McDonnell Douglas F-15I Eagle aircraft.[58] In the planning and preparation of the assassination, there was collaboration and coordination in the sharing of data and analysis among and between many Israeli politicians, military leaders, military units, and different intelligence services and their units, including the IDF Units 504, 8200, and 9900 and the ISA/Shin Bet. Individuals involved in the decision making included the prime minister, Benjamin Netanyahu, who was also minister of defense at the time; the Security Cabinet; the ISA director; and the IDF chief of staff.[59]

Active defenses including targeting infrastructures and people fall under the definition of preventive or preemptive acts. The objective is to weaken and disable the adversary as far as possible for threat reduction but not to engage in a way that might escalate to a full-scale war.[60] Gaining the upper hand in the cyber battle terrain by targeting the attacker is no different to that of the kinetic battle terrain. The outcome of the mission is impacted by successful situational awareness or the mapping of the battle terrain. It is knowing the adversary's capabilities that determines successful threat reduction through targeting. In cyber, self-awareness of capabilities is essential in order to overcome the inherent advantages that an attacker might have. Two examples are anonymity or hiding in a global network across national sovereignty and jurisdiction boundaries and forensics or the volatile and transient nature of evidence of their location that complicates analysis.[61]

Resolving this also assists in determining the motive and so the response

to a cyberattack, which might not be politically motivated even if the target is government or military. An attack could be by a seasoned criminal, a random malicious venture, or even a local citizen without prior malicious intent. Yet, a single cyberattack could cause strategic and even tangible security damage. The process of targeting is to confirm the attacker as a premeditated serial terrorist and to assess whether targeting would result in collateral damage.

Even when the attacker has been identified and confirmed as a member of a terrorist group and their location determined, it is not a foregone conclusion that targeting can be implemented. For example, in 2005 Israel implemented a unilateral withdrawal from Gaza. Hamas took the governance in an election but continued to use terror, launching rockets and incendiary balloons across the border. There was a dramatic increase of cyber hacking attempts and virus attacks by individuals in these groups, apparently only using personal computers linked to commercial internet providers by telephone modems. One option was for the IDF to have responded by destroying the buildings in Gaza, where some individuals were operating, but there was no guarantee that others would not have taken their place. Or that Hamas and its state sponsor Iran would not have escalated the conflict with rockets and missiles. This was an extension of the other battle spaces because Iran is the main financier, weapons provider, and ideological force behind Hamas in Gaza and Hezbollah in Lebanon. Therefore, the best solution for the IDF was the defensive mode.[62]

The catalyst that enabled the option for active defense and targeting came from successful cyber terrain mission mapping, digital surveillance, and monitoring. To actively defend a mission in cyberspace, efforts were taken to understand and document that mission's dependence on cyberspace and cyber assets. This is known as cyber terrain mission mapping. For example, nonstate groups in Gaza were detected in 2006 as working with the cyber warfare units of sovereign states, Syria, and Iran. It meant that for the first time the IDF could plan and prepare to implement cyber strategies against specific military cyber targets of significance in these states. The battle terrain was mapped for potential targets that would also be in proportionality to a cyberattack against Israel, as required by international laws and customs.

Although there was speculation in the media of both sides cyber attacking each other, there was no official data or confirmation. Normally, cyber warfare is conducted secretly and anonymously. There is no good reason to expose one's identity or claim or deny responsibility, as it would almost certainly result in a response. In most cyber cases, identifying the source of the attack is difficult, and so escalation is avoided. The attacker operates from afar, secretly, while defenders focus on securing the cyber space.[63] With this understanding of the risk of being identified and leading to an escalation, the IDF operates in the defensive mode in cyber.

The Organizational Infrastructure of Civil-Military Relations for the Cyber Battle Threat

There are three distinct periods in the evolving IDF cyber organizational infrastructure that when examined show how the cyber battle space and threat evolved to the significance of being assessed as equal to that of conventional, subconventional, and nonconventional. The first period was 1993–2003, the second period was 2004–13, and the third period was from 2014 to present. This section examines the periods that were concurrent with subconventional threat campaigns as well as peace processes.

The periods will be examined for a consistency in CMR for all four battle threats and for the tendency to use the defensive mode as routine and not to initiate in combat unless necessary, as political rather than military options are proffered by the civilian government and by extension of the process of CMR, also in the IDF. In the first two periods, there were the same two evaluations by the IDF: one on weaponized information and the other on cyber that confirmed this defensive mode. Events in 2014 were a catalyst to placing cyber on an equitable level with the other threats. In 2020, cyber plans, policies, preparations, training, tactics, and strategies were put to the test.

The First Period, 1993–2003

The first period evolved from the 1980s with the advent of computers in soldiers' homes connected by modems over telephone lines to the internet. There was a potential for damage from viruses infected from the internet and transferred by portable media, such as floppy disks, from their systems to the IDFs'. An example of two events highlights the threat. One of these was the global cyberattack in 1988 by Cornell University graduate student Robert Morris using the Morris Worm. Another was in 1993, when John Arquilla and David Ronfeldt, political scientists from the Rand Corporation, published an article "Cyberwar Is Coming!," which foresaw a deep change in the structure of military organizations, with the expected frequent occurrence of cyberattacks.[64]

The IDF undertook two evaluations to determine if the decades-old Israel-Arab conflict could become a digital or electronic battlefield.[65] The first was on weaponizing information. Between 1994 and 2003, there was no evidence to suggest that influencing Palestinian public opinion using propaganda, psychological warfare, information warfare, political warfare, or even disinformation would have any value on influencing Palestinian leadership.[66] At the same time, there was no evidence that Israel's adversaries would have any impact on the public opinion of Israeli citizens or soldiers, even during the Second Intifada.[67]

The second evaluation was concurrent and focused specifically on cyber, for example computer hardware devices, computing software, and computer

networks. There was apprehension that in the cyber realm, known terrorists or even individual anarchists could cause substantial disarray and even damage. Israel, in conjunction with other countries, and in a partnership of government, military, and the private sector took to identifying any emerging challenges. A long list was compiled that included individuals hacking into bank computers, organized crime, and extremist terrorist groups—some state sponsored as well as rogue states.[68]

There was a real concern given the growing use of computerized equipment in the IDFs' control, command, communications, and intelligence units (C3I). The conclusion was that if cyberattacks were successful then data could be stolen, corrupted, altered, or destroyed. A virus could freeze IDF operations. Having identified and classified cyber as a weapon, for all intents and purposes, led in 1997 to the establishment of the "Tehila Project" (Government Infrastructure for the Internet Age). It worked with global partners to envisage scenarios and prepare to counter them.

The emphasis was on defending systems and in particular isolating them on a separate network not connected to publicly accessible networks, per se fencing protection, in the same military notion of the physical fencing of the state's borders that had been taken for conventional and subconventional purposes.[69]

One cyber threat scenario became reality in 2002 with the first significant global cyberattack. It was the targeting of 13 domain name system (DNS) root servers around the world, in a distributed denial-of-service attack (DDoS), which assaulted the entire internet with a flood of data and slowed it down to a stop. Email was not delivered and websites could not be opened.[70]

Defending against cyber threats following this DDoS attack in 2002 were classified on the level of countering serious terror events. It led to the establishment of the Israeli Information Security National Authority (ISNA) within the Israel Security Agency. It was tasked with gathering information and supplying professional guidance on computing and computer infrastructure security to both the private and the public sectors to protect against threats of crime, terrorism, espionage, and exposure.

Working with the IDF, the ISNA identified one highly prioritized threat to the kinetic military forces. That was the vulnerability of computer-aided navigation and early warning systems (EWS) integrated into computerized platforms. These rely on precise satellite-based global positioning system (GPS) and timing. The serious joke went as follows: "Question: How can the enemy destroy an entire squadron of F-15 aircraft? Answer: By hacking into the airborne refueling aircraft and changing its GPS location—it won't find the squadron, no refuel, and the F-15s will fly into the sea." The solution was technologically akin to defensive protection. The Israel Aerospace Industries (IAI) developed an

advanced GPS antijamming navigation system to defend against GPS-denying systems that block communication between aircraft and satellites.[71]

The Second Period, 2004–2013

In 2004, a newer generation of IDF generals undertook new evaluations of the same two topics: weaponized information and cyber, for example computer hardware devices, computing software, and computer networks. The adversaries were the same, but technology was evolving. In part, the evaluation on weaponized information was also instigated by the sign of the times of the American military engagement in Iraq with its "winning the hearts and minds" psychological operations.

The IDF found that effectiveness of weaponized information as being limited as it would not bring an end to hostilities in the asymmetrical confrontation in the subconventional battle space and threat against terrorist groups such as Hamas and Hezbollah. Nevertheless, the Operations Branch of the IDF general staff opened experimentally the Center for Consciousness Operations (*Malat* מל"ת) at the end of the Second Intifada in 2004. It reported to the Operations Branch (in terms of command) and to the Military Intelligence Directorate (from a professional perspective).[72] The initial intent of the creation of Malat was to support kinetic operations in times of emergency and war. It became operational for this purpose in the Second Lebanon War (2006) but had very little functionality as there was a lack of preconceived plans.[73]

Part of the evaluation on weaponized information entailed examining cooperation with the various security organizations, such as the police, MAGAV, and ISA on the growing popularity of social media. During this period was the advent of Facebook in 2004, Twitter in 2006, and Instagram in 2010. It was found that social media could increase the fog of war; for instance, during an asymmetrical conflict where civilians could be motivated into civil unrest and demonstrations where they lived in the same buildings in Gaza as terrorists who did not wear uniforms, thereby making it hard to ascertain who was a combatant and hence respond with military force.

Radicalized individuals and groups could also use such social media across international borders in an attempt to change civilians' opinions and motivate them to take militant action. This could have led to an escalation involving Muslim populations within Israeli cities. Although it did not happen, a scenario entailed blocking social media as it would not have been possible to effectively manage cyber social battles, especially as disinformation could be conveyed and widely distributed.

Such disinformation could also have had an effect on IDF soldiers' morale as they were also using social media. The best solution determined was to warn

Israeli citizens and soldiers not to rely on information provided by social media and not to provide information on themselves that could cause harm and damage, in the same manner that the average person would not advertise their credit card number.[74]

On the basis of these evaluations, the use of the Malat unit was put to test in Operation Cast Lead in October 2008 in Gaza, which was a limited military campaign as an extension of counterinsurgency. This would be the first time that the IDF embarked on a combat venture with the preconceived plan to have a psychological warfare (PSYWAR) component in coordination with the tactical forces. Malat found that PSYWAR in its own right had little value as there was no evidence to suggest that influencing Gaza residents using propaganda, psychological warfare, information warfare, political warfare, or even disinformation would have any value on influencing Palestinian leadership. Conversely, it could impact the success of kinetic operations by delivering specific messages to certain Hamas fighters and units broadcast using different types of media. After the operation, when the kinetic forces returned to base, so did the psychological warfare unit.[75]

The takeaway from this was that it was possible to communicate directly with individual adversaries. However, in a reciprocal manner, it was also possible for the adversaries to communicate directly with Israeli citizens and IDF soldiers and to steal data from their computerized devices that were using the internet. For instance, fourth-generation cell phones and tablets met this description and were added to the list of desktop computers and laptops that posed an increased cyber threat to the IDF. Soldier's movements could be tracked if the cell phone's systems were hacked, for example. This was hard to resolve and tackle as every soldier on every base and every citizen, maybe from the age of four, were using cyberspace in all aspects of life, including banking, education, booking travel, ordering takeout food, and watching news channels. Clearly it had become impossible to separate the daily life of the whole country from the cyber life of physical computerized devices and computerized networks, and it blurred the distinctions between the software and applications, including social media applications and the delivery of weaponized information and propaganda.

To ensure both active and passive defensive measures, a National Cyber Initiative was set in motion and led in August 2011 to the establishment of a National Cyber Bureau in the Prime Minister's Office. Being located within the top level of the political hierarchy, it was intended to be a coordinating bureau or "strategic roof" for all relevant cyber and weaponized information affairs. Data on potential critical threats could pass up to it from many organizations, be evaluated, and if needed shared with others throughout government. For

example, if a threat was identified and had economic implications then all parts of government working in trade, industry, and commerce could be informed to improve national preparedness.[76]

In the IDF, enhanced cyber units were established to enable it to implement participation with the various security organizations. None of these units had an offensive mode as a routine task for cyber operations against any adversary. Their main task was gathering data, analysis, and protection. For example, the IDF Cyber Bureau was created within Unit 8200, one of the three main units in Intelligence (*aman* אמ"ן) and is responsible for collecting signal intelligence and code decryption. It works with Unit *Hatzav* (חצב), which collects open-source intelligence, including radio, television, newspapers, the internet, listening posts in Israeli embassies abroad, information from the tapping of undersea cables, and Gulfstream jets with electronic surveillance equipment. A Cyber Defense Department was also created within the command, control, communications, computers and intelligence (C4I) Directorate "tasked to thwart intelligence attacks and prevent disruptions and damage to components of the IDF's [*sic*] computing system, doctrinally defined as security comparable to the securing of IDF bases."[77]

To be sure the evolution of technology has meant that *command and control* (C2), a term used in the military around the world before computing has progressively had more added to the extent that it is now C6ISR—command, control, communications, computers, cyber defense, combat systems and intelligence, surveillance, and reconnaissance (ISR).

The Third Period, 2014–Present

In 2014, two events led to cyber being reexamined and reassessed and then elevated to be equal to the conventional, subconventional, and nonconventional battle spaces and threats. This was both reactive and proactive to ensure that cyber would be granted the due attention in recognition of its threat level.

The first was Operation Protective Edge in Gaza, a limited subconventional military campaign to combat counterinsurgency against Hamas in July.[78] The second event was the deteriorating relationship between the Israeli prime minister Benjamin Netanyahu and the American president Barack H. Obama over the Joint Comprehensive Plan of Action, known more commonly as the Iran nuclear deal. In Israel's view, it was not a good deal to prevent Iran from attaining nuclear capability and so posed a potential nonconventional threat. The IDF saw all the threats and battle spaces being intricately linked as Hamas was Iran's proxy and both were increasingly engaged in cyberattacks. There was the perceived necessity for IDF enhanced cyber preparedness to supplement and complement similar preparedness in the physical battle spaces as an escalation in one could lead to an escalation in all.[79]

This led Prime Minister Netanyahu to announce in 2014 that "I have decided to establish a national authority for cyber affairs, which will take care of the cyber defense of Israel. Not only for the defense of important installations and defense facilities, but also to protect the citizens of Israel from attacks."[80] The role and mission of the National Cyber Security Authority as the executive arm of the National Cyber Bureau would be to "evaluate and to formulate defensive responses to cyberattacks, including the handling of cyber events in real time, but wouldn't per se engage in any offensive operations."[81]

The wording had an emphasis on defense, indicating the political echelons saw a continuum in the defensive mode that was extended in consistency in CMR to the IDF who created a separate cyber branch to consolidate all of Israel's cyber capabilities.[82] Both the IDF and security organizations would work together with private contractors, some of whom had served as conscripts in IDF cyber units or similarly in the security organizations. For example, Israel Aerospace Industries created an online cyber academy to train on a cyber security simulator, the TAME Range Trainer. A broad range of cyber security scenarios are simulated and accompanied by exercises, lessons, and field implementations that provide trainees a real-time picture of the nature of the attack.[83]

The chief of the General Staff of the IDF, Eizenkot, confirmed the new status of cyberspace and threats as being significant and equal to the others and as being a continuum of them in CMR with a preference to the defensive mode as routine in two publications. The first was in the 2015 *IDFs' Strategy Document* that informed of the IDFs' engagement in planning, preparation, training, and defense to meet all threats including cyber where an "escalation in one battle space could also be, or lead to, an escalation in others, especially if the adversaries were the same."[84]

The second publication in 2018 was an article authored and published by Eizenkot, where he located "cyber as the fourth of battle threats along other weapons and spaces of operation, namely land, sea, and air. The three other battle threats are conventional (state), sub-conventional (non-state) and non-conventional."[85]

The first known and significant instance of the IDFs' cyber planning, policies, equipment, training, tactics, and strategy were put to the test was in 2020. This may be attributable to the success of the defensive mode where for years no significant attack was successful. In any conflict, an attack on essential civilian infrastructures is considered a serious and maybe existential event. Israel awoke to the news on 24 April 2020 that it was under cyberattack at several points against the national water system and attributed it to Iran, though it was not confirmed by them.[86]

For the first known time, in direct response to a state-based cyberattack assumed to be Iran, the IDF responded with a cyberattack against infrastructure

at the Iranian port in Bandar Abbas on 9 May 2020 and declared that it was the IDF attack.[87] This was in direct response to Israel's national water system having had been attacked on 24 April and attributed it to Iran. The target was proportional and appropriate to convey a deterrent message that if critical infrastructure is attacked, Israel will respond in kind.[88]

This exchange of cyber fire was exactly that, and it served as a warning shot that a cyberattack on essential infrastructure would be reciprocated. To ensure that the message was being conveyed, Eizenkot's successor as chief of the General Staff of the IDF, Lieutenant General Aviv Kochavi, announced on 19 May 2020 that the IDF "will continue using a variety of military tools and unique combat methods to harm the enemy."[89]

Such a statement served to bring the attack and counterattack into public mass media focus and attention, a rare occurrence for cyber. In doing so, Israel woke up on 21 May 2020 with tens of thousands of mostly unsecured Israeli websites attacked, allegedly by Iran-based hackers, who disabled the sites and replaced them with a threatening message.[90] On 28 May 2020, Yigal Unna, the head of the Israel National Cyber Directorate, defined the situation as a "turning point" in the history of Israel's cyber warfare.[91]

Conclusions

What lessons could be taken away from the hypothesis and case studies? The hypothesis is that there is consistency of CMR in Israel. It is the same democratically elected civilian leadership that determines who are the adversaries and why. It is the same IDF that implements the decision of the civilian government when the military option is made as a process and procedure of CMR. The security concept has three basic pillars: deterrence, early warning, and decisive defeat. The broad purpose of Israel's strategy is the deterrence of aggression and the clear-cut defeat of the enemy if deterrence fails. There are three national situation levels: routine, emergency, and war. The case examined cyber as the fourth battle space and threat with conventional (state), subconventional (nonstate), and nonconventional. The four coexist with cyber on an equal level with air, land, and sea against the same adversaries. All are spaces that need to be defended and controlled.

In setting the case studies to the hypothesis, the evidence examined indicated a democratically elected civilian government consistency to prefer and determine political rather than military solutions. This was extended in CMR for the IDF to implement a defensive mode as routine and not to initiate combat unless necessary, for at the forefront of decision making were considerations of casualties. Influencing both political and military decisions in the process and procedures of the civil-military relations—that is, the debate on how to tackle the adversary—was an inability to successfully confront adversaries asymmet-

rically when using the military option. The IDF, with the professional military expertise, noted that this was both in the subconventional and cyber spaces as the adversaries were the same radical and extremist nonstate groups and terrorists. If the military option was used as an offensive, there was also the potential of an escalation from one battle space and threat that could lead to an overall escalation in all. In the process of evaluations and the debate between the civilian government and military, cyber was examined as part of the overall battle terrain and found to be equitable to others as a weapon.

No further gains could be achieved by using the full resources of Israel and the IDF, so the status quo was one of a limited war both politically and militarily as defined. It would be fair to say then that the IDF is engaged as routine in a defensive mode. The IDF is only engaged in a limited offensive mode in an emergency or an escalation to counterinsurgency in battles and war. Tactics include fencing, active defense, and preventive and preemptive actions. The IDF in general does not attack. It is normally defending, protecting, and deterring. This is the routine of the IDF.

However, the adversaries do not share the same policies with regular terror and cyberattacks against civilian, government, and military targets and using as much of their resources as possible. It would be fair to say then that they are engaged in the offensive mode in a total war.

It is also fair to say that this is now under trial. The status quo cannot be maintained eternally. A trajectory of events from the 2020 exchange of cyber fire with Iran questions whether cyber can bring any substantial gain that other weapon systems cannot. It questions whether using cyber to neutralize the pending nonconventional threat from Iran will lead to escalation. If not and if the IDF succeeds, then it might also assist in threat reduction and mitigating the subconventional threat from Iran's proxies Hamas and Hezbollah. The takeaway lesson could be that cyber as a weapon may demonstrate that nothing is set in stone.

The article concludes by noting its contribution to military studies. It has provided a hypothesis that has been examined and sustained in a case revealing new information and innovative analysis. Further research can build on the hypothesis proposed in this article. Further research can look at other cases to see if they are also applicable, such as a comparative study of cases to construct theories and paradigms and to build knowledge to enhance the study and understanding of cyber. These activities could contest this hypothesis or even offer a different one.

Endnotes

1. Yoav Zitun, "IDF Establishes New Cyber Branch," *Ynet News*, 28 June 2015.

2. אסטרטגיית צה"ל [Israel Defense Forces' Strategy Document] (Tel Aviv: Israel Defense Forces, 2015).
3. Meir Finkel, "IDF Strategy Documents, 2002–2018: On Processes, Chiefs of Staff, and the IDF," *Strategic Assessment* 23, no. 4 (October 2020): 4.
4. Gadi Eizenkot, "Cyberspace and the Israel Defense Forces," *Cyber, Intelligence, and Security* 2, no. 3 (December 2018): 99–104.
5. Finkel, "IDF Strategy Documents, 2002–2018," 5.
6. Raymond Horricks and Eyal Ben-Ari, *Military, State, and Society in Israel: Theoretical and Comparative Perspectives* (London: Routledge, 2018), 79.
7. Israel Tal, *National Security: The Israeli Experience* (New York: Praeger Security International, 2000), 67–88.
8. Yossi Arazi and Gal Perel, "Integrating Technologies to Protect the Home Front against Ballistic Threats and Cruise Missiles," *Military and Strategic Affairs* 5, no. 3 (December 2013): 94.
9. *Department of Defense Dictionary of Military and Associated Terms* (Washington DC: Department of Defense, 2019), 65.
10. Brian K. Chappell, *State Responses to Nuclear Proliferation: The Differential Effects of Threat Perception* (London: Springer, 2021), 198.
11. חטיבת כוח אדם [Manpower Division] (Tel Aviv: Israel Defense Forces, 2020).
12. מגזין "מערכות" צבא ההגנה לישראל, מהדורה מיוחדת: מלחמת אזרחים בסוריה [Maarachot Magazine Israel Defense Forces, Special Edition: Civil War in Syria] (Tel Aviv: Israel Defense Forces, 2020).
13. Shmuel Bar, "Israeli Strategic Deterrence Doctrine and Practice," *Comparative Strategy* 39, no. 4 (September 2020): 321–53, https://doi.org/10.1080/01495933.2020.1772624.
14. Ahron Bregman, *Israel's Wars: A History Since 1947* (London: Routledge, 2002), 20.
15. Jasper Frei, *Israel's National Cybersecurity and Cyberdefense Posture* (Zurich, Switzerland: ETH, 2020), 5.
16. Prime Minister Ehud Olmert's pronouncement that "a state cannot protect itself ad-infinitum," reported by Hana Levi Julian, "Olmert: A State Cannot Protect Itself Ad Infinitum," *Arutz Sheva News*, 29 June 2007.
17. Yaakov Amidror, *Winning Counterinsurgency War: The Israeli Experience* (Jerusalem: Jerusalem Center for Public Affairs, 2008), 16–18.
18. Dmitry Adamsky, "From Israel with Deterrence: Strategic Culture, Intra-war Coercion and Brute Force," *Security Studies* 26, no. 1 (April 2017): 57–184, https://doi.org/10.1080/09636412.2017.1243923.
19. *Department of Defense Dictionary of Military and Associated Terms*.
20. *Department of Defense Dictionary of Military and Associated Terms*.
21. "Foreign Terrorist Organizations," U.S. Department of State, accessed 23 March 2021.
22. "Council Decision (CFSP) 2020/1132 of 30 July 2020 Updating the List of Persons, Groups and Entities Subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the Application of Apecific Measures to Combat Terrorism, and Repealing Decision (CFSP) 2020/20," *Official Journal of the European Union*.
23. *Hearing Before the Subcommittee on Near Eastern and South and Central Asian Affairs of the Committee on Foreign Relations*, 111th Cong. (8 June 2010) (assessing the strength of Hezbollah).
24. Paul K. Saint-Amour, "On the Partiality of Total War," *Critical Inquiry* 40, no. 2 (Winter 2014): 420–49, https://doi.org/10.1086/674121.
25. אסטרטגיית צה"ל [Israel Defense Forces' Strategy Document].
26. Eizenkot, "Cyberspace and the Israel Defense Forces," 99–104.
27. אסטרטגיית צה"ל [Israel Defense Forces' Strategy Document].
28. אסטרטגיית צה"ל [Israel Defense Forces' Strategy Document].
29. Eizenkot, "Cyberspace and the Israel Defense Forces," 99–104.
30. Interview with MajGen Shlomo Gazit, former head of the Military Intelligence Directorate, at the Institute for National Security Studies, Tel Aviv, Israel, 12 December 2013, hereafter Gazit interview.

31. Elia Zureik, David Lyon, and Yasmeen Abu-Laban, eds., *Surveillance and Control in Israel/Palestine: Population, Territory and Power* (New York: Routledge, 2010), 161.
32. Padraig O'Malley, *The Two-State Delusion: Israel and Palestine—A Tale of Two Narratives* (New York: Viking, 2015), 18, 28.
33. Nachman Shai, *Hearts and Minds: Israel and the Battle for Public Opinion* (Albany: State University of New York Press, 2018).
34. Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford, UK: Oxford University Press, 2018), 168, https://doi.org/10.1093/acprof:oso/9780190204792.001.0001.
35. Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy* (Tel Aviv, Israel: Institute for National Security Studies, 2016), 12–15.
36. Yehuda Ben-Meir, *Civil-Military Relations in Israel* (New York: Columbia University Press, 1995), 6–11.
37. Charles D. Freilich, *Israeli National Security: A New Strategy for an Era of Change* (Oxford, UK: Oxford University Press, 2018), 86, https://doi.org/10.1093/oso/9780190602932.001.0001.
38. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector* (Idaho Falls, ID: Mission Support Center, Idaho National Laboratory, 2016), 4.
39. Andrew R. Wilson and M. L. Perry, eds., *War, Virtual War and Society: The Challenge to Communities* (New York: Rodopi, 2008), 192.
40. Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel* (New York: Springer, 2015), 3, https://doi.org/10.1007/978-3-319-18986-4.
41. Frei, *Israel's National Cybersecurity and Cyberdefense Posture*, 34–36.
42. Paul J. Springer, ed., *Encyclopedia of Cyber Warfare* (New York: Springer, 2017), 158.
43. Zak Doffman, "Israel Responds to Cyber Attack with Air Strike on Cyber Attackers," *Forbes*, 6 May 2019, 12.
44. Suleiman Al-Khalidi, "Israel Launches Major Air Strikes on Iran-linked Targets in Syria," Reuters, 13 January 2021.
45. Ariel Levite, *Offense and Defense in Israeli Military Doctrine* (London: Routledge, 2019), 9.
46. Sharon Afek, "Breaking the Rules and Changing the Game: When Cyberspace Meets International Law," *Dado Center Journal*, no. 3 (December 2014): 43–72.
47. Yoav Ben-Horin and Barry Posen, *Israel's Strategic Doctrine* (Santa Monica, CA: Rand, 1981), v.
48. Gazit interview.
49. Shmuel Bar, "Israeli Strategic Deterrence Doctrine and Practice," *Comparative Strategy* 39, no. 4 (September 2020): 321–53, https://doi.org/10.1080/01495933.2020.1772624.
50. Chappell, *State Responses to Nuclear Proliferation*, 198.
51. Yehoshafat Harkabi, *Fedayeen Action and Arab Strategy* (London: Institute for Strategic Studies, 1968), 20.
52. Amos Gilboa, *The Threat of PLO Terrorism* (Jerusalem: Ministry of Foreign Affairs, 1985), 12–18.
53. Said Saddiki, *Israel and the Fencing Policy: A Barrier on Every Seam Line* (Doha, Qatar: Arab Center for Research and Policy Studies, 2013), 19.
54. Shaul E. Cohen, "Israel's West Bank Barrier: An Impediment to Peace?," *Geographical Review* 96, no. 4 (October 2006): 682–95, https://doi.org/10.1111/j.1931-0846.2006.tb00522.x.
55. Nejc Kardel, ed., *Israel vs. Hamas: The Middle East in Turmoil* (New York: Nova Science Pub, 2010), 28.
56. Mitchell Bard, "West Bank, Gaza and Lebanon Security Barriers: Background & Overview," Jewish Virtual Library, accessed 5 April 2021.
57. Amitai Gilad, Eyal Pecht, and Asher Tishler, "Intelligence, Cyberspace, and National Security," *Defence and Peace Economics* 32, no. 1 (January 2021): 18–25, https://doi.org/10.1080/10242694.2020.1778966.

58. "Israel Kills Top Palestinian Islamic Jihad Militant in Gaza," BBC News, 12 November 2019.
59. Benjamin Netanyahu, "Netanyahu's Remarks at a Press Conference in a Joint Statement with IDF Chief-of-Staff Lt.-Gen. Aviv Kochavi and ISA Director Nadav Argaman at the Defense Ministry in Tel Aviv," Israel.org, video news conference, 12 November 2020.
60. Ehud Eilam, *Israel's Military Doctrine* (Lanham, MD: Lexington Books, 2018), 9.
61. Alexander Kott, Norbou Buchler, and Kristin E. Schaefer, *Kinetic and Cyber* (Adelphi, MD: U.S. Army Research Laboratory, 2015), 4–5.
62. פיקוד כוחות היבשה, פעולות כוחות היבשה [Ground Forces Command, Ground Forces Operations] (Tel Aviv: Israel Defense Forces, 2012), 5.
63. International Institute for Strategic Studies, *Iran's Networks of Influence in the Middle East* (London: Routledge, 2020), 27.
64. John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12, no. 2 (1993) 141–65, https://doi.org/10.1080/01495939308402915.
65. Khalid Walid Mahmoud, *Cyber Attacks: The Electronic Battlefield* (Doha, Qatar: Arab Center for Research and Policy Studies, 2013), 18–23.
66. David Jaeger et al., "The Struggle for Palestinian Hearts and Minds: Violence and Public Opinion in the Second Intifada," *Journal of Public Economics* 96, nos. 3–4 (April 2012): 354–68.
67. Jacob Shamir and Khalil Shikaki, *Palestinian and Israeli Public Opinion: The Public Imperative in the Second Intifada* (Bloomington: Indiana University Press, 2010), 16.
68. IBP, *Israel Internet, E-Commerce Investment and Business Guide: Strategic Information, Regulations, Opportunities* (London: Lulucom, 2007), 89–92.
69. Israel Accountant-General Office, *Aspects of "TEHILA" Project Management* (Jerusalem: Ministry of Finance, 1999), 1–10.
70. Marian Quigley, *Encyclopedia of Information Ethics and Security* (New Delhi, India: Idea Group, 2007), 128.
71. Arie Egozi, "How Israel Is Leading the Global Cyberwarfare Race," Defence iQ, 1 May 2019.
72. Amos Harel, "IDF Reviving Psychological Warfare Unit," *Haaretz News*, 25 January 2005.
73. Adib Farhadi, *Countering Violent Extremism by Winning Hearts and Minds* (New York: Springer, 2020), 45–47, https://doi.org/10.1007/978-3-030-50057-3.
74. David Siman-Tov and Ofer Fridman, "A Rose by Any Other Name?: Strategic Communications in Israel," *Defence Strategic Communications*, no. 8 (Spring 2020): 17–52, 30.
75. Ron Schleifer, הלוחמה הפסיכולוגית ב"עופרת יצוקה" [Psychological Warfare during "Cast Lead"], *Maarachot Magazine Israel Defense Forces*, no. 432 (2010).
76. Michael Raska, *Military Innovation in Small States Creating a Reverse Asymmetry* (London: Routledge, 2016), 89.
77. Dov Alfon, *Unit 8200* [In German] (Hamburg, Germany: Rowohlt Taschenbuch, 2019), 28–32.
78. Daniel Cohen and Danielle Levin, "Cyber Infiltration During Operation Protective Edge," *Forbes*, 12 August 2014.
79. Gil Baram, ההיערכות למלחמה קיברנטית [Cyber War Preparedness], *Maarachot Magazine Israel Defense Forces*, no. 456 (2014).
80. Moti Bassok, נתניהו: תוקם רשות לאומית להגנה אופרטיבית בסייבר [Netanyahu: National Cyber Defense Authority to be Established], *Marker*, 4 September 2014, 2.
81. Roni Katzir, "Government of Israel, Cabinet Decision 2444, February 15, 2015," *Dado Center Journal*, no. 4 (2015): 117–35.
82. Yoav Zitun, "IDF Establishes New Cyber Branch," *Ynet News*, 28 June 2015.
83. Shoshana Solomon, "Israel's IAI to Help Bosnia Boost Cybersecurity Via Online Training Program," *Times of Israel*, 30 September 2020.
84. אסטרטגיית צה"ל [Israel Defense Forces' Strategy Document].
85. Eizenkot, "Cyberspace and the Israel Defense Forces," 99–104.

86. Omree Wechsler, *The April Cyber-attack on Israel's Water Facilities* (Tel Aviv, Israel: Yuval Ne'eman Workshop for Science, Technology and Security in Tel Aviv University, 2020), 1–3.
87. Joby Warrick and Ellen Nakashima, "Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility," *Washington Post*, 18 May 2020.
88. Warrick and Nakashima, "Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility."
89. Lilach Shoval, "IDF Chief: Israel Uses Wide Range of Tools to Defend Itself," *Israel Hayom News*, 20 May 2020, 3.
90. "Thousands of Israeli Websites Down after Suspected Massive Iranian Cyberattack," CTECH, 21 May 2020.
91. "Israeli Cyber Chief Warns of 'New Era' in Cyber Warfare," Arutz Sheva News, 28 May 2020.