# The Israel Defence Force's cyber mindset and strategic culture, with Iran in mind


## Dr. Glen Segell

*(Professor Glen Segell (DPhil, FRGS) is Visiting Professor and Research Fellow in the Department of Political Studies and Governance at the University of the Free State, South Africa. He is also Research Fellow at the Ezri Center for Iran & Gulf Studies, University of Haifa, Israel, and Editor of The Middle East Tracker and The London Security Policy Study. He is a Member of the Editorial Advisory Boards of the Journal of European and American Intelligence Studies (JEAIS) and of Cyber, Intelligence and Security (INSS). He serves as an Executive Advisory Board Member of the International Political Studies Association Research Committee on Armed Forces and Society. He holds the rank of Brigadier-General (Reserves) and is an expert for NATO STO. His publication record can be viewed at ORCID 0000-0002-4186-2761)*




**Publication date: 10 January 2022**




## Introduction[1]

The hypothesis of this article contends that information is a weapon and that a type of information warfare is cyber. It would fair to say then that weaponized information, and especially cyber combat, exhibit common traits with other types of weapons and warfare.

In all types of warfare including cyber, an attack and an attacker are a combination of intent and means. Cyber war may be limited in an offensive role, for democratic states, as they need to follow set procedures and processes to declare war. However is a total war in a defensive role, as there are daily attacks against civilians, government, and their defence and security forces.

The case examined of this hypothesis is that of the Israel Defense Force (IDF). The IDF's main threat in 2022 is from Iran and proxy terror groups for example Hezbollah and Hamas. They wage cyber war in cyber space against Israel as an additional battle front to terrorism and that is also manifest in the land, sea, and air spaces. The IDF defends against these attacks and may also incline towards a preemptive and preventive cyber offensive against Iranian uranium enrichment facilities.

## The IDF's cyber military mindset

The laws of Israel civil-military relations, that has a democratic political system. determine that it is the civilian elected political direction that dictates who is the adversary. It is the IDF who then decides the best means of defending, deterring and if need be attacking. The IDF is deemed the professional entity with the expertise.[2] This is also the case with cyber. Israeli law grants the IDF the sole legitimate remit, as the state's armed forces, to use cyber for the purpose of attack. The law enshrines the basic principles that the state is entitled to defend its existence and its population.[3]

Cyber is a new battle space. In Israel's four inter-state wars since independence in 1948, the last was in 1973, information for the IDF was mainly a function of intelligence operations, in the gathering and

analysis of data, to support combat units. All these wars were before the Internet and social media and so didn't have a cyber component.

Israel's counterterrorism and counter-insurgency conflicts have been more protracted than the four inter-state wars, and ongoing, and do have a cyber component.[4] The same military mindset and strategic culture that is evident in counterterrorism and counterinsurgency is also evident in the cyber battle space. The cyber battlefield is as complex as the non-state insurgent and terror battlefield. Cyber networks are connected and inter-connected as are terrorist groups and networks with warlords, human and drug traffickers and more. In cyber as in these it is not always easy to determine who is the attacker and even more so the motive.

In 2022 IDF generals see cyber as a dimension of war with a warfare theater, as the fourth space, as the extension of the three physical battle spaces of land, sea, and air. All four spaces are being fought against the same adversaries. For the IDF cyber space is a dimension of the conflict against these with a warfare theater that is an extension of the physical battlefield and integral to it. An escalation in one theater and space is likely to be indicative of an overall escalation as cyber is not an independent battlefield.

## The IDF's cyber battlefield

Cyber is a true battlefield for the IDF where physical damage could and has been inflicted. Cyber is a type of true weapon. A cyber-attack is not a virtual phenomenon but bears many similarities to other types of physical attacks. It is an attempt to expose, alter, disable, destroy, steal, or gain access.[5]

For Israel the cyber threat is not random. It originates from states and terror organizations with whom it has an ongoing armed conflict. The main state threat against Israel in 2022 is Iran and its non-state proxies Hamas in Gaza and Hezbollah in Lebanon. In facing these and others such as the Islamic Jihad, the cyber threat does not exist on its own, but is one of many tiers in the network of threats that they pose.[6]

The IDF, being responsible for the overall national security of Israel, has developed cyber offense and defence capacity as part of its arsenal. IDF cyber capabilities are integrated with overall strategy and tactics.[7] There are nevertheless some unique features for example determining how to respond to a cyber-attack, where international law is a factor.

International law and customs recognize an armed response to an armed attack, for the purpose of defence and preventive and preemptive strikes. However, the proportionality of response to a cyber-attack is a disputed factor. In cyber if a countries bank system were attacked, how could it proportionally respond to the attacker? And if the attacker were to be an individual terrorist but operating from another country? Would any response against an individual in another country violate its sovereignty? Would this lead to an escalation in other spaces and battle theatres?

This limits the propensity of the political echelons to grant the IDF the general authority of immediate response in cyber operations. Or even the authority to attack targets of opportunity, in preemptive or preventive operations. A miscalculated cyber offensive, or one against the wrong source and cause, could result in an escalation that might not be in cyber space, for example full conventional war.[8]

Further in strategic terms any Israeli conventional weapons or cyber-attack on Hamas and Hezbollah is limited in scope, as both these groups don't have any significant infrastructures that if destroyed would weaken them in any way. So cyber offenses are few and far between by the IDF. But that doesn't mean that the adversaries don't cyber-attack Israel daily. An example of an IDF response wasn't cyber but was an air strike on the building housing Hamas cyber attackers in 2019.[9]

## The IDF's cyber strategic culture

Historically the IDF strategic culture is status quo passive defence rather than offence.[10] An example is building security fences on the borders with neighboring states to counter insurgents. By extension into cyber the same mindset is to have Israel's essential government and military computer infrastructure fenced off from the more public networks. Similarly, as the adversaries are the same as in the physical sphere, the offensive strategy in cyber is an extension of physical counter insurgency. As with targeted assignations of terrorists, the IDF engages in pinpoint hacker strikes and occasionally penetrates the cyber space of adversaries to weaken and disable them.[11]

Such cyber strategic culture has evolved with two distinct periods for IDF cyber preparations. The first covers the period 1993 to 2004, and the second 2005 to 2015. These periods were concurrent with counter-terror and counter-insurgency campaigns as well as peace processes.

In each period there were the same two evaluations, one on weaponized information and the other on cyber. Events in 2020 with Iran put to test the plans, policies, preparations, training, tactics, and strategies. This is ongoing into 2022 and escalating.

### The first period 1993-2004

The first period started in 1993 and evolved until 2004. Globally there was a growth of desktop computers owned by individuals in their own homes and connected by modems over telephone lines to the Internet. Israel, its military, and its citizens were targeted first with propaganda, and then as technology evolved to also include computer viruses and attempts to hack into military, government, and civilian networks.

There was a real concern given the growing use of computerized equipment in the IDF's control, command, communications, and intelligence units ($C^3I$). The conclusion was that if cyber-attacks were successful then data could be stolen, corrupted, altered or destroyed. A virus could bring down the entire country or freeze IDF operations. The IDF identified and classified cyber as a weapon for all intents and purposes and cyber defence was prioritized.

This 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. One became reality in 2002 with the first significant global cyber-attack. The targeting of 13 Domain Name System (DNS) root servers around the world, in a denial-of-service attack (DDoS), assaulted the entire internet for an hour.[12]

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 (ISA also known as Shin-Bet or Shabach). It was tasked to gather information and to supply professional guidance on computing and computer infrastructure security to both the private and the public sectors, against cyber threats of crime, terrorism, espionage, and exposure.

One highly prioritized project was navigation. Already known then and ever more so as the years progressed was the vulnerability of computer aided navigation, and early-warning systems (EWS) integrated into computerized platforms. These rely on precise satellite-based positioning (GPS) and timing. The Israel Aerospace Industries (IAI) and Honeywell Aerospace developed an advanced GPS anti-jam navigation system to defend against GPS denying systems that block communication between aircraft and satellites.[13]

## The second period 2005-2015

In 2005 Israel implemented a unilateral withdrawal from Gaza, leaving it autonomous. The terrorist group Hamas took the governance of it. There was a dramatic increase of cyber hacking attempts and virus attacks using personal computers linked by commercial Internet providers. The IDF took to defending Israel's cyber space for any offensive could at best destroy the buildings in Gaza, from where individuals were operating.

A potential change arose when non-state groups in Gaza were detected working with the cyber warfare units of sovereign states, Syria, and Iran. This was an extension of the physical conflict space because Iran was the main financier, weapons provider, and ideological force behind Hamas in Gaza and Hezbollah in Lebanon. Iran was not only enhancing its cyber capability with significant infrastructures but was also making bellicose threats against Israel's very existence.[14]

In the cyber defence and offense planning similar questions were asked to the three physical battle spaces. For example, if Hamas cyber attacked and if Israeli responded, in proportionality in cyber, including against its sponsor Iran would this lead to an escalation in the physical battle spaces, for example rockets and missiles?

The IDF generals' military mindset and strategic culture towards counterterrorism and counterinsurgency came to the fore and decided to operate in all four battle spaces as one conflict. This led to a limited military campaign as an extension of counterinsurgency, Operation Cast Lead (2008) in Gaza. And this would be the first time that the IDF embarked on a military venture with a psychological warfare (PSYWAR) plan devised by a designated unit in coordination with the tactical forces.[15]

In examining lessons from this and with the potential for growing threats a National Cyber Initiative was set in motion. It led in August 2011 to the establishment of a National Cyber Bureau in the Prime Minister's Office. It's role and mission were to create a "strategic roof" for all operational units providing cyber defense (IDF, ISA, Israel Police etc.) and to operate a Computer Emergency Readiness Team (CERT-IL). It was tasked to coordinate all relevant cyber defense information, and to share it

with all parties in the economy in a manner to improve national preparedness for dealing with cyber-attacks.[16]

In the IDF, enhanced cyber entities were established. The procurement, the equipment and the training were both for the defence and the offence. The IDF Cyber Bureau was created within Intelligence Unit 8200 and became responsible for collecting signal intelligence (SIGINT) and code decryption. It works with Unit Hatzav that collects open-source intelligence (OSINT) including radio, television, newspapers, the internet, listening posts in Israeli embassies abroad, the tapping of undersea cables, and Gulfstream jets with electronic surveillance equipment. Also created was a Cyber Defense Department, within the C4I Directorate, tasked to thwart intelligence attacks and prevent disruptions and damage to components of the IDF's computing system, doctrinally defined as "security," comparable to the securing of IDF bases.[17]

During this period the mass use of social media became popular with the advent of Facebook in 2004, Twitter in 2006 and Instagram in 2010. The IDF opened social media units to monitor, initiate and respond, sometimes anonymously. Israeli citizens and soldiers were warned not to provide any information on these that could cause harm, in the same manner that the average person wouldn't advertise his / her credit card number.[18]

In 2014 all the cyber structures and units were reviewed. There were two catalysts to the review. The first was Operation Protective Edge in Gaza, a limited military campaign in extension of counterinsurgency against Hamas.[19] The other was the deteriorating relationship between the Israeli Prime Minister Benjamin Netanyahu and the American President Barak Obama, over the Joint Comprehensive Plan of Action (JCPOA) known commonly as the Iran nuclear deal. The combined Iran threat and the limited military operation against its proxy Hamas saw the necessity for enhanced cyber preparedness, to supplement and compliment similar preparedness in the three physical battle spaces.[20]

This led Israel's 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."[21]

The role and mission of the National Cyber Defense Authority (NCDA) as the executive arm of the National Cyber Bureau (NCB), was to formulate national situation assessments in the field, identify threats and attacks, direct, operate, and execute as needed all defensive efforts at the national level, based on a systemic approach, to allow a full and ongoing defensive response to cyber-attacks, including the handling of cyber events in real time.[22]

Within a few months IDF Chief of Staff Gadi Eizenkot announced, the creation of a "cyber branch" within the IDF to consolidate all of Israel's cyber defence and offense capabilities into a single fist. It would encompass all operational capacities pertaining to cyber warfare.[23]

## Year 2020 and 2022 vision

In 2020 was the first significant time known to the Israeli public that the cyber planning, policies, equipment, training, tactics, and strategy were put to the test. Israel awoke to the news on 24 April 2020

that it was under cyber-attack at several points. The attacks were against the national water system and attributed to Iran. At one facility, there were unusual data and "irregularities." At another, a pump was disconnected from automatic mode (controlled) and put into continual operation, while at another water source, the operating system was taken over.[24]

For the first known time, in direct response to a state based cyber-attack from Iran, the IDF responded with a cyber-attack against infrastructure at the Iranian port in Bandar Abbas on 9 May 2020.[25] This early 2020 exchange of cyber fire was exactly that, and a warning shot that a cyber-attack on essential civilian infrastructure would be reciprocated and be proportional. To ensure that the message was being conveyed the IDF Chief of Staff 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."[26]

This served to bring the attack and counterattack into public mass media focus and attention, a rare occurrence for cyber. Tit-for-tat and 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.[27] On 28 May 2020 Yigal Unna, the head of Israel's National Cyber Directorate, defined the situation with Iran as a "turning point" in the history of Israel's cyber warfare.[28]

## Conclusions

As a conclusion what lessons could be taken away from the hypothesis of this article and the case? The case examined the cyber military mindset and strategic culture of the IDF. For the IDF cyber is a weapon. In setting the case to the hypothesis, cyber was examined as part of a larger security threat.

Cyber for the IDF is the fourth battle space, as a dimension of war with a warfare theater that is an extension of the three physical conflict and battle spaces (air, land, and sea) against the same adversaries. It is the same IDF and IDF generals for all four spaces. All the evidence examined showed that the political echelons, and by extension in civil-military relations, the IDF prefers defence over offense.

It was shown that cyber is a total war in a defensive role, as there are daily attacks, posing a significant threat. There is a civil infrastructure that works with the IDF in defence. However, the IDF has sole legitimate remit for offense as cyber is a true weapon that can cause damage and take lives. Until 2020 cyber was perceived as a limited war, in an offensive role, as the adversarial non-state groups and terrorists couldn't be drastically affected by an IDF attack. That coupled with the pragmatism that a cyber offense against them couldn't attain a cessation of hostilities in the three physical battle spaces.

Yet it is also fair to say that the anonymity of cyber space, with minimal escalation in the past, and hence the IDF's military mindset, strategic culture, tactics, and strategy are now under trial. Until early 2020 the desire and willingness of a democratic state, Israel to wage cyber war as an offensive war was constrained and not viewed as productive.

A trajectory of events from the 2020 cyber-attack by Iran, the cyber-attack response by the IDF, and the counter-response by Iran, all on civilian infrastructures, may demonstrate that nothing is set in stone. A cyber offensive on Iranian uranium enrichment facilities in 2022 may be a more effective option than

an air strike with bombs and missiles. And it may be undertaken without risking Israeli Air Force crews over heavily defended sites a long distance from Israel.

While Iranian uranium enrichment is an existential threat there are also other threats. The question at the start of 2022 is whether any substantial cyber gain over Iran, would also bring a victory, or even an amelioration, with the Iranian non-state proxies Hamas and Hezbollah. And these pose the real daily threat and danger to Israel's civilians in their terrorist attacks including rockets, incendiary balloons, stabbings, shootings, hit-and-run traffic attacks and more.

## Notes:

[1] Another article on this topic is Glen Segell "Consistency of Civil-military Relations in the Israel Defense Forces: The Defensive Mode in Cyber" *Journal of Advanced Military Studies*. Volume 12 Number 1 Spring 2021, pp. 86-111
[2] Yehuda Ben-Meir, *Civil-Military Relations in Israel* (New York: Columbia University Press, 1995)
[3] Ariel Levite, *Offense and Defense in Israeli Military Doctrine* (London: Routledge, 2019)
[4] Yaakov Amidror, *Winning Counterinsurgency War: The Israeli Experience* (Jerusalem: Jerusalem Center for Public Affairs, 2008)
[5] Andrew R Wilson and M L Perry, *War, virtual war, and society: the challenge to communities*, (New York, NY: Rodopi, 2008)
[6] Charles D. Freilich, *Israeli National Security: A New Strategy for an Era of Change* (Oxford: Oxford University Press, 2018)
[7] Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel* (New York: Springer, 2015)
[8] Sharon Afek, *Breaking the Rules and Joining in - On the Encounter Between Cyberspace and International Law* (Tel-Aviv: Bein Haktavim, 2014)
[9] Zak Doffman, "Israel Responds to Cyber Attack with Air Strike on Cyber Attackers," *Forbes*, May 6, 2019.
[10] Yehoshafat Harkabi, *Fedayeen Action and Arab Strategy* (London: The Institute for Strategic Studies, 1968)
[11] Ehud Eilam, *Israel's Military Doctrine* (Lanham, MD: Lexington Books, 2018)
[12] Marian Quigley, *Encyclopedia of Information Ethics and Security* (New Delhi: Idea Group, 2007)
[13] Arie Egozi, "How Israel is leading the global cyberwarfare race," *Defence iQ*, May 1. 2019
[14] The International Institute for Strategic Studies, *Iran's Networks of Influence in the Middle East* (London: Routledge, 2020)
[15] Ron Schleifer, *Perspectives of Psychological Operations (PSYOP) in Contemporary Conflicts* (Brighton: Sussex Academic Press, 2013)
[16] Michael Raska, *Military Innovation in Small States Creating a Reverse Asymmetry* (London: Routledge, 2016)
[17] Dov Alfon, *Unit 8200* (Hamburg: Rowohlt Taschenbuch, 2019)
[18] David Siman-Tov and Ofer Fridman, "A rose by any other name? Strategic communications in Israel," *Defence Strategic Communications 8*, (Spring 2020): 17-52
[19] Daniel Cohen and Danielle Levin, "Cyber Infiltration During Operation Protective Edge," *Forbes*, August 12, 2014
[20] Gil Baram, "Cyber war preparedness," *Ma'arachot* 456 (2014)
[21] Moti Bassok, "Netanyahu: National Cyber Defense Authority to be Established," *The Marker*, September 4, 2014

[22] Roni Katzir, "Government of Israel, Cabinet Decision 2444, February 15, 2015," *The Dado Center Journal* 4, (2015)
[23] Yoav Zitun, "IDF establishes new cyber branch," *Ynet*, June 28, 2015
[24] Omree Wechsler, *The April cyber-attack on Israel's water facilities* (Tel-Aviv: Yuval Ne'eman Workshop for Science, Technology and Security in Tel Aviv University, 2020)
[25] Joby Warrick and Ellen Nakashima, "Officials: Israel linked to a disruptive cyberattack on Iranian port facility, *The Washington Post*, May 19, 2020
[26] Lilach Shoval, "IDF chief: Israel uses wide range of tools to defend itself," *Israel Hayom*, May 20, 2020
[27] C. Tech "Thousands of Israeli Websites Down after suspected Massive Iranian Cyberattack," *Calcalist*, May 21, 2020
[28] Arutz Sheva Staff, "Israeli cyber chief warns of 'new era' in cyber warfare," *Arutz Sheva News*, May 28, 2020