UNIVERSITÀ
DEGLI STUDI
FIRENZE

RESEARCH PAPER
FEBRUARY 2022

FROM KINETIC TO CYBER ATTACKS AND BACK: THE ISRAELI APPROACH TO DETERRENCE IN CYBERSPACE AND THE MULTI-DIMENSIONAL THREAT OF HAMAS

BEATRICE GORI

Center for Cyber Security and
International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

FROM KINETIC TO CYBER ATTACKS AND BACK: THE ISRAELI APPROACH TO DETERRENCE IN CYBERSPACE AND THE MULTI-DIMENSIONAL THREAT OF HAMAS

Beatrice Gori

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Paper

February 2022

ABOUT THE AUTHOR

Beatrice Gori is a MA student in International Relations at the University of Florence. She graduated in Political Science at the same university with a final dissertation on the Assad's power in Syria. She published for Pandora Rivista, the Italian Center for Strategy and Intelligence (CISINT) and the Center for International Studies (CeSI). She has recently become research assistant at the Institute for Counter-Terrorism of Herzliya in Israel. Her main research interests are security and geopolitical dynamics of the Middle East and North Africa (MENA) area, and she is currently doing her final thesis concerning Hezbollah.

Abstract

This paper focuses on the analysis of the increasing Israel's reliance on cyber tools in order to face Hamas and other non-state actors and the implications in terms of security strategy. The Israeli-Palestinian conflict has partly translated into the new dimension of cyberspace, unregulated and more accessible to a plurality of new actors. This resulted in a transformation of the security strategy of Israel moving in an offensive-deterring posture and in the use of cyber space as an additional battlefield. Following the clashes of May 2021 and the poor results in terms of enhancing stability, this paper concludes that Israel is carrying out a cyber low-intensity conflict right at its home front, which is increasing insecurity.

FROM KINETIC TO CYBER ATTACKS AND BACK: THE ISRAELI APPROACH TO DETERRENCE IN CYBERSPACE AND THE MULTI-DIMENSIONAL THREAT OF HAMAS

Introduction

The 11-days-escalation of violence between Israel and Hamas in May 2021 have ignited once again the region of Middle East, revitalizing the attention of the international community and world media. However, the conflict never shut down. The Middle East has experienced a pervasiveness of conflicts between state actors and irregular groups (Gaub 2015, Finaud 2019). According to Van Creveld (1991), the last large-scale conventional conflict fought in the region was the Yom Kippur/October War of 1973 between Israel and the Arab coalition led by Egypt and Syria. The conflict of 1973 specifically marked for Israel the last war fought for the affirmation of the Jewish state in the region and, after that, confrontations between national armies had become rare. Already since 1945, and exclusively after 1973, the most predominant form of conflict in the region was that of low intensity conflicts (LICs) (Van Creveld 1991).

A low-intensity conflict (LIC), i.e., a small-scale conflict that often takes place in third-world regions and which involves very rarely regular armies on both sides (Van Creveld 1991), between Israeli military forces and Islamic militias never really stops for decades and more recently, unconventional weapons such as cyber tools have been largely used. In the regional context, the cyber component is particularly relevant not only in the framework of the outbreak of ground violence, but also in the period that anticipated the conflict. As an attempt to contain the threat coming mainly from non-state actors, Israel envisaged an offensive military strategy using a combination of conventional and unconventional weapons (Eizenkot 2015). In this, cyber tools are designated to support defensive and offensive operations on all levels both in war and emergency situations (Eizenkot 2015).

This paper aims at analyzing the increasing reliance that Israel has on cyber tools in its security strategy against the threats stemming from non-state actors. We refer to the Israeli-Palestinian conflict, switching from the statehood perspective into a hybrid one in which a nation-state competes with an irregular group (Bekkers, Meessen, and Lassche 2019). Hamas is not indeed the legitimate authority in the Gaza Strip but specifically it controls the territory since 2007 (Shapira 2012). After the 2006 evacuation of Israeli military forces from the Strip, a violent conflict broke out and the terrorist group Hamas took over the Palestinian National Authority (PA), the organism in charge of the control of the territory according to the Oslo Agreements of 1993 (Shapira 2012).

In the first part of the paper, we analyze what consists of the strategy of Hamas. We also provide some significant empirical evidence that preceded the escalation of violence as part of the strategy used both by Israel and Hamas. We consider the transformation of Israeli national strategy in a deterring perspective focusing on the importance of low-intensity conflicts and their transposition into cyberspace. Then, we focus on the role of cyber issues in the kinetic escalation of violence during the month of May 2021 to show how the security strategy of Israel based on the defensive-deterring approach may not be effective in enhancing stability.

We rely on the approach of authors such as Dunn Cavelty (2012, 105) according to which cyber component are increasingly relevant in conflict because of the high vulnerability of critical infrastructures. Therefore, though considering hyperbolic the visions of an “electronic 9/11”, or “cyber-Pearl Harbor”, we recognize the fundamental role of cyberspace in modern conflicts. At this regard, Demchak (2012) has introduced the term “cybered conflict”, in opposition to the debated “cyber war”, to refer to the pervasiveness of cyber technology in all the activities of life. Among the opponents to the concept of cyber war, Thomas Rid (2012) is one of the most influential. Rid (2012, 142) affirmed that cyber war cannot take place in the form of violence and death but in other forms that cannot be considered proper war, e.g., espionage. At this regard, he also advanced that cyber conflict can reduce the amount of violence between states. As Stone (2013, 103) argued, Rid associates war only with death and lethal violence and this can result misguiding. If instead, recalling his argument, we use the Clausewitz’s definition of war as “an act of physical force”, a cyber attack can be defined an act of war if it involves violence as the capacity to cause physical damages (Brantly and Van Puyvelde 2019, 151).

The spread of power struggle into cyberspace requires a redefinition of the concept according to the peculiar characteristics of this domain. Kuehl (2009, 39) defined "cyberpower" as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power." Disposing of power in cyberspace and manifesting superiority in a cyber conflict is related to the ability to use, to deny but also to protect, this environment. Referring to the defense concept, we can rely on the work of Arquilla and Ronfeldt (1993) in which, almost three decades ago, they defined Information and Communication Technology (ICT) as increasingly crucial in our societies and thus capable of make them more likely to disruption. Considering the vulnerabilities of states to cyber threats, during the last two decades, states have been forced to enhance their systems of defense. As Nye (2010, 3) remarked, the physical and the digital layers of cyberspace overlap and therefore, a comprehensive defense approach cannot be possible without including the virtual domain. Israel provides examples of a sophisticated cyber "fortification" in which cyberspace occupies a crucial role for the operativity of all the domains (Eizenkot 2015).

The reasons of the peculiarity of the Israeli case are twofold: even if it collocates in the general trend of cyber build-up of powers, Israel has adapted the resort to cyber tools on the conflictual neighboring context in which it stands and, thus, it had combined this within its strategic thinking.

Israeli Strategic Thinking

In order to understand how the reliance on cyber tools fits into the Israeli strategic thinking, it seems useful to briefly analyze some of the cornerstones of the military doctrine. The strategic thinking of Israel had been covered under a veil of secrecy until the very last few years. In fact, the Israel Defense Forces (IDF) released their first public defense doctrine only in 2015 (Eizenkot 2015). In this IDF document, some of the principles that have driven the security strategy of the state since its born are clearly remarked: deterrence, early warning, defense, defeating the enemy, and victory (Eizenkot 2015). The origins of these strategic principles can be traced both on the structural characteristics of the state itself and also on the struggle for the affirmation of the Jewish state in the region and the conflictual dynamics stemming from it (Giles 2002). Due to its tight territories (i.e., 22,000 km^2 in a long and narrow shape), Israel has limited resources and does not dispose of strategic depth which results in a defensive-deterring posture (Giles 2002, 2). At this regard, the IDF's official doctrine affirmed the necessity, especially with the nearby threats such of Hamas and Hezbollah, both of reducing the capability of the enemies to attack the Israeli home front, e.g., destroying their forces, and dissuading them from attacking again proving Israeli valuable results (Eizenkot 2015).

Throughout the decades, Israel has tried to enhance its physical borders with material barriers (Jager 2021), such as the Israel-Gaza barrier and avoid ground wars within its borders in order to prevent enemies from any territorial gain and defend its physical integrity (Eizenkot 2015). Therefore, the military leading conception is to fight and win short wars because even one defeat could mean a compression of territories (Shapira 2015). Additionally, the long experience of high-intensity wars with the Arabs until 1973[1] has contributed to shape two main strategic streams: the "conflict orientation", i.e., conquering as territories as possible to enhance Israeli capability, and the "peace orientation", i.e., avoiding as wars as possible and strengthen Israel in a democratic path which includes negotiations with the Arabs (Giles 2002, 5-6). Between these orientations, a third one, the "security orientation" (ibid.) seems to be the more appropriate for the XXI century's scenario. The security orientation is based on the necessity of a defensive posture as indispensable for the survival of the state and found its fulfilment in the recent IDF national security strategy.

The maintenance of a defensive posture is one of the programmatic goals included in the IDF multi-year strategic doctrine of 2015, including this concept of defense tied with an offensive military view: enemies cannot be defeated with a defensive posture and therefore the use of force is necessary to obtain military results (Eizenkot 2015). The implementation of this strategy has been facilitated by the employ of

[1] At this regard, the Yom Kippur War/October War of 1973 had an enormous impact: it was the longest war that Israel ever fought – it lasted one month – and the then Prime Minister Golda Meir was forced to demand to the USA immediate military supplies (Shapira 2015).

sophisticated technologies (Kober 2015). Since the use of cyberspace for military purposes has become concrete, Israel rushed on the creation of its own cyber weapons arsenal coherently with its priority to dispose of a technologically advanced defensive system. An acceleration in terms of Israeli transformation of weaponry derived from the regional context. Beside Iran, Lebanon and Syria, non-state actors represent the main enemies of Israel, and they rely a lot on cyber capacities (Eizenkot 2015). The increasing reliance to cyber weapons by Hamas and Hezbollah shaped the security strategy in terms of systems of defense and offensive operations (Eizenkot 2015; Frei 2020). Israel engaged in low-intensity conflicts with Hamas and Hezbollah (Kober 2015) in which the employ of cyber tools has become central. Low-intensity conflicts have always been pervasive in the military history of Israel (Kober 2016). The difference now, as we will see with some empirical evidence, is the large resort to cyber weapons, which poses serious problems in terms of uncertainty as in the recent events of May 2021.

The resort to non-conventional tools in a framework of low-intensity conflicts resulted in a radical transformation of the structure of IDF. In order to explain the reasons underlying this transformation, we can relate to the approach made by Avi Kober (2015) and its adaptation of the post-heroic concept coined by Luttwak (1995) concerning the post-Cold War geopolitical scenario. Kober (2015, 99) refers mainly to two ideas of post-heroic: the willing to reduce casualties among the own troops and the necessity of avoiding civilian deaths. In this view, it pertains to a less disposal to the war sacrifice coming both from the society[2] and the militaries themselves. Additionally, this switch in priorities helps democratic states to be coherent with themselves when going to war. Israel tried to switch into this direction long time ago, since the 80s and the "Lebanese swamp" represented by the Lebanese Civil War (Libel 2011, Kober 2016). In particular, the period 1975-90 – which coincides with the Lebanese Civil War – have globally represented the failure of conventional forces (Van Creveld 1991).

A strong change in IDF structure and doctrine can be traced from the First Lebanese War in 1975 and the Second Lebanese War of 2006 (Libel 2011). Along this time horizon, Israel constantly dealt with informal groups, badly armed as the case of the first Intifada in 1987 where the Arabs were "armed" just with stones. Beforehand, these low-risk

[2] Concerning this, Levy (2012) focused on that he made on the impact of the movement of *Four Mothers* in shaping the idea of a need of security for soldiers in Israel.

threats, i.e., contentious violent events but also borders incidents and terrorist attacks, were considered simply occasional. The contentious movements of Intifadas showed that a conventional ground war as that happened in 1973 was remote and the new threat derived from irregular actors (Libel 2011). The use of a “heroic”, traditional approach in those situations would cost thousands of civilian deaths as well as severe urban destruction. A structural change which involved specialized training and weapons was necessary: counterinsurgency squads were completely different from high-intensity conflicts’ battalions (Libel 2011).

The Militarization of a *Fortified* Cyberspace

In the Israeli official security doctrine, the maintenance of the superiority in terms of technological capabilities and intelligence is one of the fundamental national goals (Eizenkot 2015). With its sophisticated military and intelligence technologies, Israel has one of the most advanced cyber security apparatus in the world,[3] ranking globally in the first ten countries in terms of offense and intelligence capabilities in cyberspace (Voo et al. 2020). The primary objective of Israel has been the cyber defense: the cyber “fortification” of Israel started in the 90s with the aim of protecting information and sensitive data (Tabansky 2013).

The term “fortification” refers to the translation of the Israeli paradigm of the use of force, – as we have seen before: deterrence, early warning, defense, defeating the enemy, and victory – from the physical domains to the cyber one in order to strengthen IDF capabilities in the whole war theatre. In fact, cyber domain has been included in the multi-dimensional defense together with land, air, and sea (Eizenkot 2015).

If the cyber build-up of Israeli civilian infrastructures has started well before, the first cyber unit of IDF saw the light in 2011 (Jager 2021, 18)

[3] According to the National Cyber Power Index (NCPI) elaborated by the Belfer Center, in 2020 Israel is ranked in the eleventh place for comprehensive cyber power (Voo et al., 2020, 11). If we see in detail the various components of the index, we note that Israel collocates globally at the fifth place for cyber intelligence apparatus and for information control and at the third for cyber offence capabilities (31). Moreover, Israel is one of those countries that did not fully disclose publicly all its cyber resources, and this means that it could appear lower than it actually is (16).

on the wave of the global phenomenon of "militarization of cyberspace", based on the belief in a massive threat of a large-scale cyber attack (Dunn Cavelty 2012, 114). In fact, since Stuxnet[4] and the evidence of the possibility to be targeted by states-sponsored cyber weapons, states have enlarged their military activity – simply defensive or also offensive – to the domain of cyberspace. In the Israeli case, the scenario of a destructive cyber attack is concrete as the IDF systems are based on networking and a cyber attack could prevent their effective operability. In the IDF strategy, cyber defense in wartime and during emergency situation has been defined "vital to enable operation of state institutions and (…) the effective operation of the IDF" (Eizenkot 2015). More general, most of Israeli facilities – not only military, but also civilian – have an electronic component that could be suitable of intrusions and disruptions in case of a cyber attack (Cohen, Freilich, and Siboni 2016, 6), defined indeed by former Prime Minister Netanyahu as "one of the four main threats to Israel" (Barak 2014). In the 2017 National Security Strategy (INCD 2017), the exigence of a "national cyber defense" was affirmed to mitigate the threats of aggression coming both from state and non-state actors (Frei 2020).

These strategic objectives are implemented reportedly by two organizations: the IDF Unit 8200 for cyber offense and the Computer Services Directorate C41 for cyber defense (Frei 2020). These are the main bodies in charge of the military cyber realm, and they are clear examples of the Israeli sophisticated military organization translated into cyber (Cohen, Freilich, and Siboni 2016, 8).

The Unit 8200, subordinate to the Military Intelligence Directorate (AMAN), has among its major and known tasks intelligence signals, decrypting operations, and electronic warfare. Its origins have to be found in the failure of warning capabilities of intelligence in the 1973 War (Cordey 2019, 3). Since that traumatic episode[5], the Unit was enhanced and with 5,000 soldiers active on duty it became soon the largest single unit of IDF (Cordey 2019, 3). According to some authors, the Unit is the organ from which many cyber attacks have been launched and also Stuxnet is believed to have been jointly coordinated

[4] Stuxnet malware represented a watershed in the debate about the role of cyber in military. It was the first case of an offensive cyber attack that caused severe physical damages. In fact, it reportedly took out and destroyed around 1,000 centrifuges of the nuclear plant of Natanz in Iran (Brantly and Van Puyvelde 2019, 150-51).

[5] See footnote 1.

by the 8200 and the US National Security Agency (NSA) during the Operation "Olympic Games" (Cordey 2019).

IDF official website reported that recently Israel had decided to not create a Unified Cyber Command but to strengthen the C4I (Command, Control, Communications, Computers, and Intelligence) and Cyber Defense Directorate that since 2017 has a double defense and offense function: it is responsible for defending all IDF networks and communication infrastructure against attacks and it is authorized to respond to cyber attacks (Cohen, Freilich, and Siboni 2016).

Israel Defense Forces are not new in using mixed strategies of cyber realm and kinetic force (Parmenter 2013). Israel often resorted to cyber tools to support conventional military operations as in the case of operation "Orchard" in 2007, an attack against the nuclear reactor in Dayr ez-Zor, in northern Syria (Cohen, Freilich, and Siboni 2016). In this operation, the Israeli Air Force (IAF) was able to fly into the Syrian air space and bomb the nuclear plant without alerting Syrian air defenses (Fulghum 2010, 29-30). In order to do that, Israel reportedly attacked and took control of Syrian radar systems that went blind and were temporarily reprogrammed to make it appear that they were instead functioning normally (Cohen, Freilich, and Siboni 2016, 8-9).

The idea to *fortify* Israeli cyberspace in a defensive/offensive posture has been recently reaffirmed by the Prime Minister Naftali Bennet during the 2021 Cyber Week Conference in Tel Aviv in which he exposed the aim to create a "global network shield" with other countries in order to collaborate and develop an "online and real time" defense force against cyber threats that will "alert, investigate, together develop a 'vaccine' and disperse the 'vaccine' to all countries in the network" (Solomon 2021).

Escalation and the Israeli Approach to Deterrence in Cyberspace

The cyber fortification envisaged by Israel has been supported by the doctrinal principle of deterrence reaffirmed also in the official national security strategy of 2015 (Eizenkot 2015). The concept of deterrence has always been an essential element of Israeli defense and refers to the aim of deterring regional adversaries proving that there is very little possibility of success in attacking the Jewish state (Bar-Joseph 1998). The concept of deterrence envisaged by Israel has completely different roots: it was not created for a specific contingency, e.g., containing Soviet expansion, and it has been present in the Jewish strategy of defense since the 1920s, from before the actual state of Israel was born in 1948 (Rid 2012, 125). Notwithstanding the long tradition of deterrence, it lacks a theoretical conceptualization and an intellectual environment as that shaped US paradigm (Bar-Joseph 1998, 147). The geopolitical scenario in which the strategy is deployed is then completely different: if the US wanted to maximize its benefits from nuclear weapons without never using them, Israel wants to postpone and limit all the unsettled conflicts around it (Tor 2017). US strategists developed the theory of deterrence in the perspective of achieving the absolute deterrence over every great power in the world preventing the threat of a nuclear attack; Israel instead never aspired to an absolute domination but to an overall strategic position in the Middle East in the perspective of restricting its enemies (Tor 2017, 94-96). This strategy was initially envisaged to deal with the threat of ground invasion by Arab states (Tor 2017). Later on, with the progressively appeasement of Arab states, the major nearby threats come from non-state actors, i.e., Hezbollah and Hamas, and terrorist organizations, e.g., Palestinian Jihad and ISIS (Eizenkot 2015). In the IDF's official document of 2015, it is noted how the Israeli basic concept of deterrence cannot be fully applied because of the different current threat (Eizenkot 2015).

Therefore, we relate to a restrictive concept of deterrence concerning the national security strategy of Israel (Tor 2017, 93). As said earlier, the domain of cyberspace is a crucial part of the security strategy of Israel but applying the Western concept of deterrence in this domain is a complex issue. Richard Clarke and Robert Knake (2010, 189) state that "of all the nuclear strategy concepts, deterrence theory is probably the least transferable to cyber war". First, it is necessary to have a clear opponent who is afraid of retaliation. Nevertheless, in cyber era the attacker is not clearly defined because of the problem of attribution (Craig and Valeriano 2016, 144). Secondly, it is fundamental to have a reliable costs-benefits estimation. In cyber domain, it is difficult for states to estimate an accurate picture of the adversary's capabilities (Craig and Valeriano 2016). In addition, cyber weapons have a high degree of uncertainty because results of operations are difficultly predictable.

Uri Tor (2017) had applied the paradigm of "cumulative deterrence" coined in 2004 by IDF Major General Doron Almog concerning war on terrorism (Almog 2004) to the Israeli strategy in cyberspace. This approach to deterrence referred to the aim to limit and postponing conflicts by constantly attacking the enemies in order to demonstrate an "overwhelming military force" (Almog 2004) and, at the same time, accepting the inevitability of receiving back some cyber attacks in what, differently from the case of nuclear threat, they cannot be fully prevented (Tor 2017, 95). Additionally, the features of the conflictual context allows Israel to get around the impossibility of applying the paradigm of deterrence by punishment into cyberspace. In the region, Israel confronted the same enemies for years: Hezbollah in the South of Lebanon, Hamas and affiliated-Jihad militias in the Gaza Strip and Iran, that supports directly or indirectly all of them. For what it concerns Arab countries, they have been never less interested in the Palestinian cause than now. Even though it is still not possible to determine with technical evidence the identity of the attacker, from a political perspective it can be assumed who it could be. Indeed, cases of physical retaliation carried out by Israel against its alleged attackers are several and they should be considered as the maintenance of a posture of deterrence. Also, the concept of self-defense in cyberspace is completely different: if an attack by land should be responded with a land attack rather than a naval one, in cyberspace it is very common to use a combination of cyber tools and conventional weapons to respond to a cyber attack (Nye 2016, 46-47). It was the case of the airstrike launched by Israel in 2019 in which an entire Hamas's building in Gaza was destroyed and that the IDF's official twitter account defined as an act of response for an alleged cyberattack (@IDF, May 5, 2019).

As Ellias Groll (2019) reported, it was the first time that a national army responded to a cyber attack with the employ of physical force. IDF affirmed that Hamas launched a cyber attack with the precise aim to harm "the quality of life of Israeli citizens" and this implies the possibility to act in self-defense (Groll 2019). It was not clear what the target was and how the IDF attributed the attack to Hamas, but it does not really matter to Israeli purposes. High-quality attribution is fundamental in an international legal framework or if you need to resort to collective response (as in the case of art. 5 of NATO) but Israel is not interested in any of that. Israel is not a member of NATO, and it has expressed a cautious position about the validity of International Law in cyberspace

(Schmitt 2020).[6] What matters to Israeli national strategy is a quotidian commitment promptly attacking back in the perspective of reducing threats and deterring its enemies, instead of obtaining an absolute and decisive triumph over the opponents (Rid 2012, 141).

Attacking adversaries during peace time has been a strategy directed also against distant enemies in order to move the tension far from its national borders. As seen during the last year, Israel has launched several cyber attacks against crucial infrastructures in Iran. Some of those attacks targeted Iranian industrial plants where drones imported to Hamas were produced (Petroni 2021). These examples are emblematic of how Israel uses cyber attacks during the “grey zone”, i.e., the period between peace and war (Nye 2016).

The Multi-dimensional Threat of Hamas

Hamas, acronym for *Harakat al-Muqawama al-Islamiyya*, literally *Islamic Resistance Movement*, has assumed a multi-dimensional nature as religious and social movement, political party, and terrorist organization (Gleis and Berti 2012, 2). Because of its heterogenous nature, it has envisaged a multi-dimensional offensive approach, i.e., a variety of illicit operations including kidnappings, infiltrations through tunnels, propaganda, in which cyberspace occupies a privileged position (Eikenzot 2015). Hamas is in fact military inferior comparing to Israel and cyberspace has offered to the Islamic militia the possibility to try to fill the military gap at an affordable price. Through cyberspace, terrorist and irregular groups can in fact elevate their power coordinating illegal activities, recruiting activists, and spreading propaganda (Brantly and Van Puyvelde 2019, 184-85). Islamic terrorists use Internet to recruit adepts and manipulate believers into terrorism in the name of Allah through the diffusion of *fatwa*[7] (Weimann 2021).

[6] The debate concerning the militarization of cyberspace also involved the international legal framework. The most critic positions are those of Russia and China that reject the applicability of international law in cyberspace and affirm the exigence to create a completely new set of rules. Israel situates in the middle of these two strains affirming the necessity to consider an extensive interpretation of self-defense (as in art. 51 of UN Charter) in case of cyber attacks not only against states but also non-state actors (Schmitt 2020).

[7] In the Islamic world, both Sunni and Shia, a *fatwa* is a religious opinion on a matter of Islamic Law, and it is common to share them on online platforms (Weimann 2021).

This explains why Hamas has invested a significant amount of resources in cyber operations (Dostri 2015). Moreover, Israel has a high degree of reliance on technology in its defensive and offensive systems (Eikenzot 2015) and, paradoxically, this made it more vulnerable to cyber attacks.

Almost a decade ago, after a cyber attack against the Israeli company of airlines El Al – which caused a Distributed Denial of Service (DDoS) and the theft of credit cards information of El Al users – the Hamas spokesman Sami Abu Zuhri said in Gaza: "this is a new field of resistance against the Occupation, and we urge Arab youth to develop their methods in electronic warfare in the face of Israel's crimes" (Lubell 2012).

More recently, in 2014, as a response to the IDF operation "Protecting Edge" in Gaza, Israeli citizens faced large-scale DDoS attacks coming from Qatar and Iran (Raska 2015). The attacks against governmental agencies such as *Shin Bet* (Israeli Security Agency) were successfully contained while against civilians they provoked some inconvenience (Raska 2015). Cyber capabilities of Hamas do not represent a major threat to Israel, and cyber operations conducted by Hamas consisted mainly in defacements and vandalism of Israeli national websites and attempts of stealing information (Dostri 2018). However, this kind of low and medium-threshold operations advise the target that its security system is failing in control and defend cyberspace (Valeriano and Craig 2015, 34).

The strategy of Hamas, and Hezbollah, accelerated the structural transformation of Israel Defense Forces, which have progressively enhanced cyber and intelligence units to strengthen the national security. In this respect, in 2018, former Prime Minister and Chief of General Staff Benny Grantz affirmed: "I prioritized cyber and intelligence over infantry and armour … unlike the threat of ground invasion, the threat of cyber is realistic" (Jager 2021, 14). Accordingly, non-state actors' threats stand as the driving forces behind the transformation of the army of Israel (Jager 2021, 16-17). If Israel has developed highly sophisticated systems resulting the most advanced army in the Middle East (Baram 2017, 3) the diffusion of conflict into the cyber domain is a double-edged sword in what it potentially means opening the gate to an increasingly plurality of non-state adversaries which will be able to threat Israeli security.

The Conflict between IDF and Hamas of May 2021

The conflict of May 2021 between Israel and Hamas, Islamic Jihad and other militant groups in the Strip have provoked approximately 250 deaths in Gaza and 12 in Israel (Arshad et al. 2021). Israel said that around 4,360 rockets were fired from Gaza and successfully intercepted by the Iron Dome[8] in the 90% of the cases; 680 of them fell instead short into the Strip (Arshad et al. 2021).

Some of the strikes launched against Gaza in the month of May were indeed oriented by cyber security concerns. In fact, the bombardments were often directed to Hamas' cyber facilities. As the IDF twitted on their official account, the first "cyber defensive operation" was on May 5 over "a building where the Hamas cyber operatives work" (@IAFsite 2021). On May 14, another strike was directed against one objective defined by the Israeli Air Force on Twitter as "a cyber-equipment storage site in the northern Gaza Strip belonging to Hamas military intelligence" (@IAFsite May 14, 2021). Just five days later, another strike hit what was defined by the IAF on Twitter as a "hideout apartment used by the terror operatives for offensive cyber activity against Israeli targets" (@IAFsite May 19, 2021). Destruction of cyber facilities is part of the "mowing the lawn" strategy adopted by Israeli intelligence with Gaza, considering any conflict with Hamas as a window of opportunity to destroy as much military facilities as possible.

In addition to the conflict that IDF were fighting at home, some cyber operations were deployed abroad. On May 23, Iran claimed to have suffered a major explosion at the petrochemical factory in Isfahan, in the central province of the country (Wintour 2021). The factory is owned by the Iran Aircraft Manufacturing Industrial Company (HESA Saeqeh) and a variety of aircraft and drones are produced there and then exported to Iranian allies such as Hamas or Hezbollah (Wintour 2021). Even though there is no possibility of attribution of the attack, the suspects are addressed mainly to Israel. The attacks to Iranian facilities are perfectly integrated in the defensive-deterring strategy of Israel. Even though the major threat is represented by enemies just alongside the national borders, Israel wants also to dissuade actors such as Iran that are sponsoring enemies at its doorstep. Moreover, attacking Iran

[8] A powerful system that can intercept rockets and destroy them before falling on the ground.

through technological facilities means also move the conflict far from its national borders. In fact, the employ of cyber tools in remote conflicts could appear a practical way to exercise power without increasing tensions right at the Israeli borders.

Conclusions

The conflict between Israel and Palestine still remains unsettled and one of the main worrying fronts for Israel is the Gaza Strip. The diffusion of conflict with Hamas and Palestinian groups into cyberspace poses a wide spectrum of new challenges for Israel.

Non-state actors rely a lot on cyber capabilities in the perspective to operate in a battlefield where they can try to compete with the Jewish State. Hybrid groups use cyberspace to conduct illicit operations and remind states of their vulnerability increasing the perception of insecurity and concerning that Hamas is considered a serious threat by the Government of Israel.

If the defensive posture envisaged by Israel against cyber attacks is fundamental, carrying on continuous offensive attacks in the framework of a deterring strategy seem more problematic. A security concern emerges as in the conflict of May 2021 in which the red line between a LIC in cyberspace and kinetic war was quickly crossed. Considering the very high number of wars with Hamas in the last decade – among them the longer was the 50-days-conflict of 2014 – it seems that instead of dissuading the enemy, this strategy could increase instability right at the home front of Israel.

Albeit the reasons that conducted to the escalations of violence are many and have to be traced also in societal and structural problems, perpetual cyber operations increased the level of tension between the parties. Additionally, each military operation whose target is Hamas' facilities in Gaza does not result only in weakening military power of the militia but also in worsening the situation of civilians in the Strip and this, besides moral concerns, means increasing the desperate living conditions in which terrorists potentially can proliferate.

To conclude, the IDF offensive-deterring strategy in cyberspace seem to be more efficient in the longer trajectory, for instance to contrast hostile measures coming from Iran that are successfully moving the conflict far from the national borders. If the concept of cumulative deterrence applied by Tor (2017) to cyberspace seems useful, a longer-term perspective should be evaluated in terms of regional stability.

Combining the multi-dimensional threat of Hamas together with the exigence of security *per se* could be the starting point for the understanding of the Israeli approach to the multi-dimensional threat of Hamas. A further analysis could consider both the role of Hamas in social issues and the terrorism methods to elaborate an operational approach to the analysis of the threat. Terrorism methods, also through cyberspace, have shown the necessity to elaborate a different approach, as they may not be successfully integrated in a defensive strategy without this *caveat*. In light of this, the Israeli paradigm of deterrence should be considered in a comprehensive framework in which terrorism methods and the strategic use of the blurred nature of cyberspace are involved. A focus on the social and economic issues should also encompass the security implications of the role of Hamas as welfare provider and the consequences in terms of reducing violence in the area.

References

Almog, Doron. 2004. "Cumulative Deterrence and the War on Terrorism." *Parameters* 34, no. 4 (Winter): 4–19.

Arquilla, John, and David Ronfeldt. 1993. "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (April): 141-65.

Arshad, Mohammed, Jonathan Saul, John Irish, and Parisa Hafezi. 2021. "Israel's Gaza challenge: stopping metal tubes turning into rockets." *Reuters*, May 23, 2021. Accessed June 30, 2021. https://www.reuters.com/world/middle-east/israels-gaza-challenge-stopping-metal-tubes-turning-into-rockets-2021-05-23/.

Baram, Gil. 2017. "Israeli Defence in the Age of Cyber War." *Middle East Quarterly* 24, no. 1 (Winter):1-16.

Bar-Joseph, Uri. 1998. "Variations on a theme: The conceptualization of deterrence in Israeli strategic thinking." *Security Studies* 7(3): 145-81.

Bekkers, Frank, Rick Meessen, and Deborah Lassche. 2019. "Hybrid Conflicts: The New Normal?" The Hague Center for Strategic Studies. Accessed October 27, 2021. https://hcss.nl/report/hybrid-conflicts-the-new-normal.

Brantly, Aaron F., and Damien Van Puyvelde. 2019. *Cybersecurity: Politics, Governance and Conflict in Cyberspace.* Cambridge: Polity Press.

Clark, Richard A., and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collins.

Cohen, Matthew S., Charles D. Freilich, and Gabi Siboni. 2016. "Israel and Cyberspace: Unique Threat and Response." *International Studies Perspective* 17, no. 3 (August):1-15.

Cordey, Sean. 2019. “Trend Analysis: The Israeli Unit 8200 – An OSINT-based study.” Center for Security Studies (CSS), ETH Zürich.

Craig, Anthony, and Brandon Valeriano. 2016. “Conceptualising cyber arms races.” 8th International Conference on Cyber Conflict (CyCon): 141-58.

Demchak, Chris. 2012. “Resilience, Disruption, and a ‘Cyber Westphalia’: Options for National Security in a Cybered Conflict World.” in *Securing Cyberspace: A New Domain for National Security*, edited by Nicholas Burns and Jonathon Price, 59-94. Washington DC: The Aspen Institute.

Dostri, Omer. 2018. “Hamas’s Cyber Activity against Israel. The Jerusalem Institute for Security and Strategy.” Accessed October 26, 2021. https://jiss.org.il/en/dostri-hamas-cyber-activity-against-israel/.

Dunn Cavelty, Myriam. 2012. “The Militarisation of Cyber Security as a Source of Global Tension.” ETH Zurich Center for Security Studies.

Eizenkot, Gadi. 2016. *Israel Defense Forces Strategy Document. Deterring Terror. How Israel Confronts the Next Generation of Threats*. English Translation of the Official Strategy of the Israel Document. Translated by the Belfer Center for Science and International Affairs. Cambridge: Belfer Center for Science and International Affairs.

Fulghum, David. 2010. “No Fingerprints.” *Aviation Week and Space Technology* 172: 29-30.

Finaud, Marc. 2019. “New forms of conflict and arms control in the Middle East: Return to the future?” Geneva Centre for Security Policy (GCSP). July 24, 2019. Accessed December 15, 2021. https://www.gcsp.ch/global-insights/new-forms-conflict-and-arms-control-middle-east-return-future.

Gaub, Florence. 2015. “Hizbullah’s hybrid posture: three armies in one.” European Union Institute for Security Studies.

Gleis, Joshua, and Benedetta Berti. 2012. *Hezbollah and Hamas. A Comparative Study*. Baltimore:

John Hopkins Press.

Groll, Ellias. 2019. “The Future Is Here, and It Features Hackers Getting Bombed.” *Foreign Policy*, May 6, 2019. Accessed October 28, 2021. https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/.

Gross, Judah Ari. 2017. “Army beefs up cyber-defense unit as it gives up idea of unified cyber command.” *The Times of Israel*, May 14, 2017.

Israeli Air Force (@IAFsite). 2021. “A short while ago, in a joint effort by the IDF Computer Service Directorate, the IDF Military Intelligence Directorate and the Israeli Air Force, an IAF fighter jet struck a cyber-equipment storage site in the northern Gaza Strip belonging to Hamas military intelligence.” Twitter, May 15, 2021. https://twitter.com/iafsite/status/1393206783389405187.

Israeli Air Force (@IAFsite). 2021. “Overnight, The IAF and the ISA neutralized three Hamas terror operatives located in an operational hideout apartment in Gaza City belonging to the Hamas cyber unit. The target was struck by IAF fighter jets.” Twitter, May 19, 2021. https://twitter.com/IAFsite/status/1395040936799965192.

Israel Defence Forces (@IDF). 2019. “We thwarted an attempted Hamas cyber offensive against Israeli targets.” Twitter, May 5, 2019. https://twitter.com/IDF/status/1125066395010699264.

Jager, Avi. 2021. “The Transformation of the Israel Defence Forces.” *Naval War College Review* 74, no. 2 (Spring): 1-25.

Kaldor, Mary. 1999. *New and Old Wars: Organized Violence in a Global Era*. Stanford: Stanford University Press.

Kober, Avi. 2015. "From Heroic to Post-Heroic Warfare: Israel's Way of War in Asymmetrical Conflicts." *Armed Forces & Society* 41(1): 96-122.

Kober, Avi. 2016. *Practical Soldiers. Israel's Military Thought and Its Formative Factors*. Leiden: Brill.

Kuehl, Daniel. 2009. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited ny Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 24-42. Washington DC: Potomac Books.

Lubell, Maayan. 2012. "Israel rattled as hackers hit bourse, banks, El Al." *Reuters*, January 16, 2012. Accessed July 8, 2021. https://www.reuters.com/article/us-israel-hackers-idUSTRE80F0V220120116.

Luttwak, Edward N. 1995. "Toward Post-Heroic Warfare." *Foreign Affairs* 74, no. 3 (May - June): 109-22.

Nye, Joseph Jr. 2010. "Cyber Power". Belfer Center for Science and International Affairs.

Nye, Joseph Jr. 2016. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (Winter): 44-71.

Parmenter, Robert C. 2013. "The Evolution of Pre-emptive Strikes in Israeli Operational Planning and Future Implications for Cyber Domain." MA Thesis, School of Advanced Military Studies at the United States Army Command and General Staff College, Fort Leavenworth, Kansas.

Petroni, Federico. 2021. "Stallo all'americana." *Limes Rivista Italiana di Geopolitica* 5. "La Questione Israeliana."

Raska, Michael. 2015. Confronting Cybersecurity Challenges: Israel's

Evolving Cyber Defence Strategy. Policy Report 8.S. Rajaratnam School of International Studies.

Rid, Thomas. 2012. “Deterrence Beyond the State: The Israeli Experience.” *Contemporary Security Policy* 33(1): 124-47.

Schmitt, Michael. 2020. “Israel’s Cautious Perspective on International Law in Cyberspace: Part II (jus ad bellum and jus in bello).” Blog of the European Journal of International Law, December 17, 2020. Accessed October 26, 2021. https://www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-ii-jus-ad-bellum-and-jus-in-bello/.

Senor, Dan and Saul Singer, 2009. *Start-up Nation: The Story of Israel’s Economic Miracle*. New York: Hachette Book Group.

Shapira, Anita. 2015. *Israel: A History*. London: Orion Publishing Group.

Solomon, Shoshanna. 2021. “Bennett: Israel to set up ‘global network shield’ against growing cyberthreat.” *The Times of Israel*, July 21, 2021.

Stone, John. 2013. “Cyber War Will Take Place!” *Journal of Strategic Studies* 36 (1): 101-08.

Tabansky, Lior. 2013. “Cyberdefense Policy of Israel: Evolving Threats and Responses.” Chaire de Cyberdefense et Cybersecurité, January 2013. Accessed October 26, 2021. http://sectech.tau.ac.il/sites/default/files/publications/article_3_12_-_chaire_cyberdefense.pdf.

Tor, Uri. 2015. “‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence.” *Journal of Strategic Studies* 40, no. 1-2 (December): 92-117.

Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press.

Van Creveld, Martin L. 1991. *The Transformation of War*. New York: Free Press.

Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy, and Anina Schwarzenbach. 2020. *National Cyber Power Index 2020. Methodology and Analytical Considerations.* Cambridge: Belfer Center for Science and International Affairs.

Weimann, Gabriel. 2011. “Cyber-Fatwas and Terrorism.” *Studies in Conflict & Terrorism* 34(10): 765–81.

Wintour, Patrick. 2021. “Blast at Iranian complex housing drone factory injures nine”. *The Guardian*, May 23, 2021. Accessed October 28, 2021. https://www.theguardian.com/world/2021/may/23/blast-at-iran-factory-as-israel-accuses-state-of-providing-drones-to-hamas.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies