JOURNAL OF POLITICAL STABILITY ARCHIVE

Online ISSN: 3006-5879 **Print ISSN:** 3006-5860

DOI: https://doi.org/10.63468/jpsa.4.2.23

Vol. 4 No. 2 (2026)

https://journalpsa.com.pk/index.php/JPSA/about

Recognized by: Higher Education Commission (HEC), Government of Pakistan

The Role of Cyber Warfare in the Modern Era: A Case Study of the Israel-Hezbollah War

Shazia Batool *
Student of International Relations, FUUAST, Islamabad
shaziabatoolwork@gmail.com

Abdul Rafay Ameen Shah
Student of International Relations, Federal Urdu University of Arts, Science, and Technology, Islamabad
rafayshah764@gmail.com

Taha Atif Bhatti
Student of International Relations at the National University of Modern Languages (NUML), Islamabad
tahaatifbhatti2004@gmail.com

* Corresponding Author

ABSTRACT

The twentieth century has seen cyber warfare emerge as a defining feature of twenty-first-century conflict, shifting the dynamics of competition between states and non-state actors in terms of power, legitimacy, and security. This paper examines the influence of cyber warfare in modern asymmetric warfare, with reference to the 2006 Israel-Hezbollah War, which was one of the first cases in which a cyber operation was combined with conventional military forces. The research focuses on the use of low-cost cyber strategies such as defacing websites, online propaganda, and mass intimidating messages by Israel to undercut the image of Hezbollah and shift public attention. To counter this, Hezbollah engaged in counter-cyber operations, such as breaking into Israeli communication networks, jamming, and holding on to their media outlets, including Al-Manar, to interfere with Israel and its propaganda so that they could continue to act as they do. The analysis highlights that the two parties

resorted to the use of cyber warfare to cause diversions and psychological pressure, thereby making the battle an information war rather than a military war. Making use of the Realist theory, this study suggests that cyber warfare in asymmetric warfare is a leveller of power, which enables weaker players to face more technologically developed states and makes states change their approaches to cyber warfare to ensure their supremacy in security. The paper finds that the Israel-Hezbollah conflict established a precedent in which cyber and conventional warfare are merged in hybrid warfare, and there is an urgent need to establish legal, political, and military frameworks to deal with the menace of cyber war in international relations.
Keywords: Cyber warfare, Israel-Hezbollah War, asymmetric conflict, hybrid warfare, propaganda, information operations.

INTRODUCTION

The development of the war in the twenty-first century is characterised by the introduction of novel technologies that do not align with the traditional conflict (Cremer et al., 2024; Pietrzak, 2024). Cyber warfare has been one of these innovations and has become a very serious field where no tanks and missiles are used, but keyboards, code, and digital platforms are used to fight the battle. Cyber war: Cyber war is the application of digital technology and computer networks to interfere, destroy or control the systems of an opponent with military, political or psychological interest (Geiß, 2006). Cyber operations are inexpensive in comparison with the large-scale military campaigns, and unlike traditional warfare, they are borderless, can be anonymous and very effective in the hands of both the state and the non-state actors.

The interdependence of contemporary societies on the network of interconnected communication systems, financial structures, and media has predisposed them to cyberattacks. The digital disruption is prone to power grids, water systems, air defence networks and government databases, and these can be used to cripple national security, interfere with social order, and influence the perception of the people (Clarke and Knake, 2010). This change brings serious questions to the essence of conflict: in the case of waging wars in cyberspace, how to establish battle lines, and what to consider as victory? (Paterson & Hanley, 2020)

An excellent example of cyber warfare being incorporated into a military conflict was provided in the 2006 Israel–Hezbollah War, which was among the earliest and most important instances of using cyber warfare. It is dubbed the Second Lebanon War, and in July 2006, Hezbollah militants violated the borders of Israel and triggered a cross-border attack that resulted in a 34-day battle that saw a lot of airstrikes, rocket fire, and ground assaults. Off the battlefield, however, there was a struggle on in cyberspace. Israel and Hezbollah capitalised on digital capabilities not only to sabotage the operations of the opponent but also to shape the local and foreign opinion. This cyber aspect was a breakthrough as compared to the past wars in the

Middle East, as it indicated a new way of fighting wars, where wars would be fought both in the physical and the cyber realms. The Israel-Hezbollah War is especially relevant as it provides an example of the functioning of cyber warfare in the asymmetric conflict between a technologically superior and an up-and-coming militant entity under unequal terms of military force. Israel is facing Hezbollah, which is a guerrilla organisation with minimal conventional power yet well-established networks and ideological credibility and the most sophisticated military and cyber security systems in the globe. In this asymmetric warfare, Hezbollah used cyber warfare as a change of direction, applying it to confuse Israel, cause panic among the population, and export its message into the battlefield. In the case of Israel, cyber warfare was part of its national defence policy, being employed to spy and disrupt the propaganda and communications of Hezbollah(Kalb & Saivetz, 2007). The psychological, informational, and operational distractions were the focal point of the cyber aspect of the Israel war with Hezbollah. Israel used affordable cyber warfare techniques such as defacements, internet propaganda, and intimidation messages on a mass scale to ruin the reputation of Hezbollah and distract the masses. In reaction, Hezbollah also implemented counter-cyber attacks, such as hacking Israeli communication systems, jamming broadcasts, and seizing their own media, and Al-Manar specifically, to counteract the propaganda of Israel and hold their own ground. These activities compelled Hezbollah to shift its interest in the battlefield to the defence of information, an example of how cyber warfare redefines the allocation of resources and concentration in the conflict scenario (Kalb & Saivetz, 2007).

The diverters produced by both parties show how cyber warfare plays a dual role in asymmetric warfare: it might not directly alter the result of a battle on the ground, but can nonetheless have a major influence on the psychological and political aspects of a war. The 2006 war demonstrated that the ability to regulate information, influence perception, and create confusion may be as decisive as physical superiority in the contemporary war. The Israel-Hezbollah War is generally recognised as one of the first examples of hybrid warfare, a policy that unites traditional warfare with irregular wartime and cyber-warfare. The cyber war (Parry, 2010) in this hybrid form does not work in isolation, but it supplements the attacks and propaganda campaigns. To Hezbollah, the use of rockets in northern Israel was complemented by Internet propaganda that enhanced the effect of the psychological consequences of the attacks. In the case of Israel, cyber attacks complemented precision airstrikes that sought to suppress the communication of Hezbollah and avoid the spread of its propaganda. This blending of the cyber and kinetic strategies made battlefields indistinguishable, thus making the war a multi-domain war (Al-Rizzo, 2013).

Theoretically speaking, the issue of cyber warfare in the Israel-Hezbollah War can be analysed in the context of the Theory of Realism. Realist theory focuses on power, security, and survival in an international system that operates under anarchy

(Mearsheimer, 2001). To Israel, cyber war was an arm of the state, employed to ensure the superiority of security and exercise control over the hostile environment. To both players, cyber actions allowed Hezbollah, though a military organisation, to question the authority of Israel, counterbalance its military weakness, and declare to the world that it was not going anywhere (Rynning, 2010). The case of Israel and Hezbollah highlights wider issues in international security. The absence of precise laws regulating cyber wars enables both states and non-state actors to act in a grey area of accountability. The attribution of cyber attacks is also sometimes hard to do, which makes weaker actors able to operate with plausible deniability using highly impactful cyber tools, disrupting traditional deterrence paradigms (Atzili, 2010). The disruption created during the Israel-Hezbollah War is an example of the increasing significance of narrative control and psychological power in the creation of contemporary conflicts.

LITERATURE REVIEW

Cyber warfare has been a critical topic of the study of security as the virtual space continues to determine the nature of conflict. Rid (2013) defines cyber warfare as politically-based hacking, as well as the application of digital instruments in the disruption, espionage, or destruction. According to the literature, the peculiarities of cyber war include its borderless character, non-costly character, and anonymity possibilities, which make it very different compared to traditional military methods (Clarke & Knake, 2010). According to scholars, there is no denying the fact that providing cyber operations as part of the state security strategies is inevitable. As an example, Nye (2010) explains cyber power as the capability to utilise cyberspace in order to realise strategic goals either through coercion, disruption or attraction. This can be conceptualised as a two-sidedness of cyber tools; they can be used to strike down an enemy and build up resilience. From the Israeli case, cybersecurity is institutionalised by the state, as it has been part of Israeli military doctrines, and has created divisions, including Unit 8200, a unit dedicated to cyber intelligence (Tabansky and Ben-Israel, 2015). On the other hand, cyberspace is also a plus to an emergent militant group. The international availability of the internet allows organisations like Hezbollah to propagate, recruit, and carry out psychological activities without necessarily having to step up to the military infrastructure (Deibert, 2013). Therefore, it can be seen in the literature that cyberspace has emerged as an area where asymmetric power relations are enacted, as this poses a threat to the traditional state-based models of war. The application of cyber warfare as an instrument of asymmetric strategy is one of the dominant ones in the literature. Asymmetric warfare is a case where weaker parties fight against the stronger parties using unconventional strategies (Arreguino-Toft, 2001). According to researchers, the cyber tools provide a potential opportunity to cyber actors to level the playing field

through the exploitation of vulnerabilities of technologically dependent countries (Kello, 2017). As an example, Arquilla and Ronfeldt (1993) refer to the concept of a netwar, the warfare when networks of actors use information and communication technologies to wage warfare, as one of the important features of the modern conflicts. Such strategies include cyber sabotage, disinformation and hacking. The examples of such approaches by Israel portray the concept of asymmetric warfare. It used digital tools to generate distractions, interfere with Hezbollah communications, and display power by spreading propaganda. It is also claimed in the literature that cyber warfare adds to the psychological operations in asymmetric wars. Thomas (2003) reveals that cyber activities are usually aimed at creating perceptions but not on physical assets, thus increasing fear and confusion. An example of this strategy was the case of Israel sending threatening SMS messages to the citizens of Lebanon in 2006. Researchers note that such cheap tactics can have massive psychological consequences, demoralising and forcing the government to act (Shachtman, 2007). There exists a large amount of literature on the enhancement of propaganda and information warfare through cyber means. Online videos, social media messages, and disinformation campaigns have turned into a means to influence the opinion and perception of the people and the international opinion. Carr (2012) emphasises the fact that propaganda is one of the first and most common applications of cyber operations by two groups, specifically the Middle East.

The Israel Hezbollah War of 2006, Hezbollah utilised its satellite television programme Al-Manar and Internet websites and online videos to air resistance stories and Israeli vulnerability (Avital, 2007). By cutting these routes with the means of cyber actions and airstrikes, Israel caused Hezbollah to turn to other online tiers, which exemplifies the strength and flexibility of digital propaganda (Lobel, 2012). Israel also entered into information warfare by attacking the communication channels of Hezbollah. Tabansky and Ben-Israel (2015) argue that using electronic warfare with cyber hacking, Israel interfered with broadcasts and also diverted internet traffic, trying to substitute the message of Hezbollah with pro-Israel information. The following distractions point to how information control was valued on par with victories on the battlefield. Some researchers have analysed the cyber aspect of the 2006 war. The war also became a watershed for hybrid warfare, where digital and physical operations were integrated. Both used defacing internet sites and hacking, anti-Zionist slogans were sprayed on Israeli sites, and Hezbollah sites were riddled with Israeli spyware. These cyber battles were not symbolic but were attempts at regulating the information stream and taking away the credibility of the opponent.

A different stream of literature is on the distractors generated by cyber operations. In Shachtman (2007), Israel is recorded to have sent thousands of SMS messages and emails warning the Lebanese citizens of further attacks, and causing fear. The civilians were diverted through this psychological warfare, and the Lebanese

government was pressured, which reflects how digital tools can be used to increase the social cost of a conflict. Hizbollah, in its turn, upset the propaganda of Israel, as it shut down its websites, compelling the organisation to invest in protecting its information infrastructure (Avital, 2007). The literature, therefore, highlights the dual purpose of cyber operations: as offensive instruments to disturb the enemies and as defensive instruments to control the threat. This dynamic shows that the war of 2006 was not in the physical realm but in the realm of cyberspace, as an information war. Cyber warfare has led to concern about how to deter and regulate internationally. Formal deterrence theories are based on attribution and punishment, and cyber operations do not have these characteristics. As the case of Israel and Hezbollah shows, it is possible to address how an up-and-coming militant organisation can implement effective operations with no fear of punishment. According to this challenge, creating new types of deterrence that would be technologically resilient and reflect the international legal frameworks proves to be challenging due to the issues of attribution and proportionality (Lindsay, 2013). During the Israel-Hezbollah war, on several occasions, it was not clear whether the cyber attacks were the direct brainchild of Hezbollah or Israel to alter the dynamic of the war. Likewise, the fact that Israel interfered with the communication of Hezbollah posed a question as to whether the act of attacking media houses during wartime was legal. There is an agreement in the literature that international law has failed to respond to the reality of cyber conflict. Although not binding, the Tallinn Manual (Schmitt, 2013) is one of the initial efforts to enforce international law on cyberspace. Nevertheless, cyber warfare, as the case of Israel-Hezbollah demonstrates, exists in areas of law and politics where the responsibility fades into grey.

METHODOLOGY

The research design that will be used in this study is a qualitative research design based on a case study. The focus on qualitative research is suitable since it will not be possible to measure the number of cyber operations but comprehend their meanings, approaches, and consequences within the framework of contemporary wars (Creswell, 2014). The approach of the case study allows for the study of the Israel-Hezbollah War of 2006 in detail as a distinct but notable case of cyber warfare that was incorporated into a traditional one. There are two reasons as to why this design has been selected. First, the Israel-Hezbollah War is one of the most documented and first cyber wars waged in the Middle East. Second, analysing the case study will enable the incorporation of several pieces of information, published literature, news articles, policy documents, and even online archives to create a comprehensive picture of the cyber aspect of the conflict (Yin, 2018). Through this conflict, the study determines the use of cyber operations and the disruption they caused, as well as the overall implications of the same to international security.

Data Collection

Use of secondary data sources is based on the study, and they include:

1. Academic Literature:

Scientific articles, books, and conference proceedings would give conceptual and analytical theories of cyber warfare. The theoretical basis is informed by other scholars like Rid (2013), Nye (2010, 2017), and Kello (2017), although case-specific works like Al-Rizzo (2013), Tabansky and Ben-Israel (2015) inform the context of the conflict between Israel and Hezbollah.

2. Reports: Policy Documents:

Articles by non-profit agencies, think tanks, and government agencies (e.g., the RAND Corporation, NATO documents, and the Tallinn Manual) are also reviewed in an effort to see the way norms and policies on cyber warfare are developed and changed.

3. Media Sources and Archival Records:

The analysis of newspaper publications, broadcast texts, and online archives in 2006 was conducted to track particular cyber attacks, including website defacements, propaganda campaigns, and countermeasures. The New York Times, Haaretz, and Al Jazeera sources give real-time coverage of cyber and psychological operations on the conflict.

4. Digital Evidence:

The files of websites that are defaced, screenshots of propaganda, and documented cases of SMS intimidation campaigns are utilised to explain the strategies that are utilised by both Hezbollah and Israel. These are limited because of the lapse of time, but archival information regarding researchers on cybersecurity is still available (Shachtman, 2007).

The triangulation of these sources helps the research to minimise bias and have a holistic picture of the cyber aspect of the war.

Data Analysis

This information is discussed with the help of a qualitative thematic approach, which determines common patterns and themes regarding cyber warfare in the conflict between Israel and Hezbollah. The discussion will be informed by the empirical data and theoretical knowledge of Realism. The analytical framework is informed by three themes:

1.The Cyber Warfare as a Distraction:

The attention of the enemy was diverted, confusion was caused, and morale was undermined through the cyber tools employed by Israel and Hezbollah. As an example, the SMS intimidation campaigns of Israel are encoded under psychological distraction, and the SMS attacks of Hezbollah on the Israeli websites, together with defending its Al-Manar television channel against hacking.

2.Asymmetric Strategy- Cyber Warfare:

It was a matter of how Israel, being an advanced state in terms of technology and limited in areas of law, fought cyberwar with an up-and-coming militant group, Hezbollah. This theme explores the propaganda spread, web defacements and psychological activities.

3.Cyber Warfare as State Power Project:

The ways Israel integrated cyber activities into its larger military and intelligence practices and employed hacking, spying and jamming in order to dominate. This theme underscores the way states use cyber tools to be offensive and defensive.

The information is systematically checked, and examples of certain cyber incidents are inserted in these themes. The interaction between cyber and kinetic activities is also discussed in the analysis and shows how digital tools were incorporated into the hybrid warfare.

4.Reliability and Validity

This study compares data with various independent sources to find out the reliability. As an example, the cases of defacing websites are supported by cybersecurity records and press releases. On the same note, the records of Israel's interference with the television station of Hezbollah are substantiated by news archives and policy studies. The validity is provided through the location of the findings on existing theoretical and empirical constructs. By joining the analysis with the Realist theory, the paper explains cyber warfare not as technical accidents but as tactics that are in line with the quest to gain power and survival.

Case Study and Analysis

The history of Israel and Hezbollah conflict goes as far back as the early 1980s, when Israel invaded Lebanon in 1982 and occupied the southern part of Lebanon. Such a job was generally considered illegal based on international law, and this caused opposition among the locals. It is against this backdrop that Hezbollah, which is sponsored by Iran and is supported by parts of the Shi'a population in Lebanon, has become an opposition group whose main agenda is to oust the Israelis from Lebanese territory. During the 1980s and 1990s, Hezbollah resorted to guerrilla warfare, ambushes and rocket attacks against Israeli troops and positioned its struggle as a liberation struggle. Meanwhile, Israel continued to have the security buffer region in southern Lebanon, citing a case of protecting its settlements in the north. But it was long Hezbollah opposition, coupled with rising international condemnation, coupled with pressure in Israel, that eventually caused Israel to pull out its troops in southern Lebanon in May 2000. The retreat was perceived as a big triumph by Hezbollah, and this increased its credibility in Lebanon as well as in the rest of the Arab world.

Even after the withdrawal, there were still tensions over the disputed territories, including the Shebaa Farms, and Hezbollah continued to militarise. These incomprehensible matters prepared the ground for the direction of the confrontation

again, with the result of the 2006 Israel-Hezbollah war. On July 12, 2006, the war started after Hezbollah crossed into northern Israel with a cross-border raid and seized two Israelis. The war also led to the death of over 1,200 in Lebanon and approximately 160 in Israel, with tremendous displacement and devastation of infrastructure (Biddle and Friedman, 2008). In addition to the usual military interactions, the 2006 conflict was one of the first examples of hybrid warfare, as cyber and psychological operations were introduced on the battlefield. Israel and Hezbollah utilised cyberspace to have a perception, propagate propaganda, and de-motivate their opponents so that the war became not only a battle of territory but also a battle of narratives (Al-Rizzo, 2013).

1. Cyber Operations of Hezbollah

Being a young militant organisation with little military capability relative to Israel, Hezbollah used cyber tactics to gain strength and confront the traditional forces that Israel had. The cyber activities that Hezbollah carried out in 2006 can be divided into defacements of websites, propaganda, psychological threats, and cyber attacks.

2. Website Defacements

Being affiliated with Hezbollah, hackers defaced several Israeli government and commercial sites to showcase the conflict. The anti-Israel slogans and Hezbollah symbols were usually found on the defaced pages (Shachtman, 2007). Such defacements were symbolic, yet highly effective because they showed that Hezbollah could enter Israeli digital space and humiliate the state with the help of weakening its cyber resilience. The defacements also defocused the Israeli authorities as they had to devote their technical resources to restoring websites and not only to concentrate on military activities.

3. Propaganda Campaigns

Hezbollah widely applied digital propaganda to exude power and durability. Videos of victorious rocket attacks, photographs of shattered Israeli tanks and speeches made by Hassan Nasrallah were very common on the internet, especially on websites, forums, and online networks (Avital, 2007). When Hezbollah was struck or interrupted by Israel by bombing or jamming its Al-Manar satellite television broadcasts, the group moved on to internet platforms, thus its message of resistance could be reached (Lobel, 2012). This flexibility made the internet a battlefield of legitimacy, and Hezbollah entered the fray against Israel to influence the opinions of the region and the world.

4. Attempted Hacking and Disruption of Information

The hackers, who are also affiliated with Hezbollah, wanted to gain access to Israeli communication systems and databases. Despite the high-capacity cyberdefense of Israel due to the sophisticated cybersecurity systems, the ongoing attempts compelled the Israeli defence agencies to be on the alert, which overstretched their cyber defence ability (Tabansky and Ben-Israel, 2015). Such operations showed how

Hezbollah used cyberspace as a low-budget but high-impact area of asymmetric warfare.

5. Israel's Cyber Operations

Israel, which has a highly developed tool in cyber tool, incorporated cyber operations into its overall military strategy in the 2006 war. These were aimed at interfering with the communication of Hezbollah, crippling the propaganda machine, and also to collect intelligence by using cyber surveillance.

6. Al-Manar Television interference

Israeli cyber and electronic attacks were constantly used on al-Manar. Israel also blocked satellite transmissions and closed down the internet streaming of Al-Manar as a way of curbing the freedom of Hezbollah to broadcast its account of the war (Avital, 2007). Israel wanted to ensure Hezbollah was not focused on the field of battle and its popularity among followers, which is why it targeted the media outlet.

7. Hacking of websites and redirection

Israeli cyber teams invaded Hezbollah websites, substituting the content with pro-Israel messages or redirecting the users to sites that revealed connections of Hezbollah to terrorism (Shachtman, 2007). This brought about a narrative war on cyberspace because Hezbollah wanted to re-establish its digital image, while Israel was using the loopholes in messaging. The attacks prompted Hezbollah to allocate resources to digital defence, and the focus was taken out of the military campaigns.

8. Cyber Warfare and Jamming of Communication

The sophisticated electronic warfare tools used by Israel interfered with the radio communication of Hezbollah, compromised its command and control, and created confusion among the warriors on the battlefield (Al-Rizzo, 2013). These operations not only thoroughly diverted the leadership of Hezbollah but also impaired coordination, which undermined guerrilla tactics.

9. Cyber Intelligence and Surveillance

In addition to direct attacks, Israel employed cyber intelligence to track the activities of Hezbollah, intercept communications, and track financial networks (Tabansky and Ben-Israel, 2015). Surveillance had strategic value in exposing the supply channels and plans of operation by Hezbollah. The espionage ability highlighted the fact that Israel incorporated cyber weaponry in its strategy of warfare, which augmented its traditional superiority over its digital superiority.

Diversions Made on Each Side

The peculiar character of cyber warfare in the 2006 Israel-Lebanon War was the application of it as a means of distraction and manipulation of the psyche.

Hezbollah's Distractions

- Defacements of websites were an embarrassment to Israel as the organisation would reveal its weaknesses in its cyber infrastructure.

- SMS intimidation campaigns helped to focus the attention of civilians, causing fear and disruption of normal life.
- Videos of ruined Israeli tanks were used as propaganda that made international watchers not focus on the defeat of the Hezbollah troops at the battlefield, perceiving the war as won by the resistance.

Israel's Distractions

- Israel neutered Hezbollah by shutting down Al-Manar TV and hacking the websites of Hezbollah, which made it not focus on the battlefield, but it had to protect its propaganda networks.
- Jamming communications was used to cause disorientation of the Hezbollah fighters at a vital time on the ground.
- Cyber intelligence enabled Israel to attack first, enabling the Hezbollah leadership to divert attention through the abrupt defeats and blocked plans.

These interruptions explain how cyber warfare has blurred the demarcation between psychological and military activities. To Hezbollah, digital diversion made up for the military inferiority. In the case of Israel, internet diversions strengthened its military strategy by undermining the Hezbollah authority in its own territory and communication.

Analysis

The cyber aspect of the 2006 war is an example of hybrid warfare, in which cyber warfare and conventional warfare supplemented each other. Hezbollah not only used rocket attacks and refrained from propaganda, but also made sure that every physical attack was doubled with the help of the internet. Israel combined airstrikes with cyber repression of the media of Hezbollah, in an attempt to diminish the effect of the Hezbollah narrative of opposition. In this perspective, cyber warfare acted not as a battlefield but as a multiplying agent. The distractions that were formed by both parties extended the psychological aspect of the war and ensured that it was not only fought on the ground but also in the minds of civilians and the global observers.

DISCUSSION

The 2006 Israel-Hezbollah War highlights the increasing significance of cyber warfare in asymmetric warfare, where non-state groups face technologically advanced states. The conventional tools of power, the number of troops, air domination, and hi-tech equipment, are being augmented by the means of information and perception control. The cyber activities of Hezbollah showed that low-cost and easily available digital technologies can help an emerging militant group to have a strategic impact that is not commensurate with its material capabilities (Shachtman, 2007).

Israel increased its impact and diverted the Lebanese society with battlefield results through defacements, propaganda spread, and SMS threats, by use of websites. These strategies are logical approaches to asymmetric warfare: weaker parties do not

want to face more powerful ones, but rather attack at the psychological level and capitalise on the reliance of contemporary society on digital connections (Arreguín-Toft, 2001). The cyber operations in Israel added weight to this dynamic by outlining the reaction to asymmetric threats by states. Israel tried to deny Hezbollah the informational space that it needed to mobilise support by jamming the communications of Hezbollah, disrupting the Al-Manar broadcasts, and hacking the propaganda websites. What transpired was a cyber war that involved the two sides developing distractions that influenced the perceptions of the war, which can be described as the spread of asymmetric strategies into cyberspace.

The Cyber Warfare Role of Distractions

Among the greatest contributions of the conflict of 2006 was that it proved that distraction is one of the major roles of cyber operations. Distractions, in this case, mean trying to distract the opponent and confuse them, and affect the morale of the civilians.

Distractions were force multipliers for Israel. The SMS intimidation campaign, as an example, shifted the focus of the Lebanese civilians from military resilience to personal insecurity. The defacements on the websites brought embarrassment to Israel on the international front, distracting Israel from its losses on the battlefield. On the same note, online propaganda reinterpreted Hezbollah as a movement of rebellion and triumph that did not focus the international community on the traditional military supremacy of Israel (Avital, 2007). In Israel, distractions were a source of traditional power. The media break-up of Hezbollah compelled the organisation to invest funds in online counter-defence instead of fighting the organisation. Jamming of communications also disrupted Hezbollah fighters at the most crucial times of fighting. Through the use of cyber intelligence, Israel could predict and frustrate the schemes of Hezbollah, which added another dimension of psychological and operational disorientation (Tabansky and Ben-Israel, 2015).

Such twofold efforts demonstrate that cyber distractions were not even side effects but conscious plans, part of the wider military and political plans. The Israel-Hezbollah War, therefore, points out the fact that distraction is not a byproduct of cyber war but a characteristic mechanism by which cyber operations have had a strategic impact.

Cyber Warfare Through the Lens of Realism

Theoretically, the contribution of Realism is a good source of information about the contribution of cyber warfare to contemporary wars. Realism underlines that power, survival, and security are the key areas of focus of the states that act in the anarchic international system (Mearsheimer, 2001). Although Realism was traditionally used to analyse the interstate relations, it can also explain the conflicts involving other new actors, such as Hezbollah, that act in a strategic manner in order to increase their survival and power.

The cyber activities in Israel can be summarised as follows: being a state, Israel has applied its technological advantage to its security hegemony, silencing its opponents, as well as insulating its people against psychological attacks. The cyber tools turned into a means of state power and strengthened the military of Israel, indicating the possibility of acting in different spheres. Although Hezbollah was a new actor, it operated on the principles of Realism. Hezbollah resorted to asymmetric warfare, such as cyber attacks, to counter the superiority of Israel. Through propaganda displaying strength, spreading fear to Israeli civilians, and causing distractions that undermined the legitimacy of Israel, Hezbollah sought to survive and exert power based on its limited resources (Al-Rizzo, 2013). The Realist paradigm highlights the fact that cyber warfare, like any other type of conflict, is ultimately power politics and the survival quest. Both traditional weapons and cyber weapons, actors are interested in improving their security, influencing the project, and weakening the enemy.

Hybrid Warfare and the Seamlessness of Borders

The other theme that comes out during the discussion is the issue of cyber warfare in hybrid strategies. Hybrid warfare describes a combination of traditional, irregular, and cyber warfare into a single operation (Hoffman, 2007). The Israel-Hezbollah conflict proved that cyber operations are not singular events but a part of the bigger strategies. Airstrikes by Israel were also accompanied by cyber sabotage of the media of the Hezbollah group, undermining their capacity to legitimise themselves. The rocket attacks staged by Hezbollah were intensified with the help of online propaganda, and so the physical attacks had disproportionate effects on psychological effects. Such interconnections erased boundaries between the physical and digital battlefields that formed a hybrid conflict indeed. According to the literature, the future conflicts will be characterised by hybrid warfare as both states and non-state actors will add cyber tools to their arsenals (Kello, 2017). The Israel-Hezbollah War is therefore a forerunner of modern wars, where online activity cannot be separated from the traditional military attack.

Consequences to International Law and Security

The conflict of 2006 also indicates essential issues of international law and security. Cyber operations are in a grey zone of the law as opposed to traditional warfare. Websites, defacements, propaganda, and communication jamming cannot be easily classified under the current armed conflict laws. The issue of attribution is also a focus: commonly, there is uncertainty on whether the cyber attacks are instigated by state officialdom, proxies, or individuals (Nye, 2017). As an illustration, although most cyber activities during the war were linked to Hezbollah, the decentralisation of cyberspace has increased the chances of the presence of sympathetic groups or even outside parties. In a similar manner, the fact that the actions of Israel, by targeting the media of Hezbollah, are viewed as legitimate military targets, rather than illegal

assaults on civilian facilities (Schmitt, 2013). Lack of an agreement on cyber norms also makes it difficult to control such conflicts. The Tallinn Manual is the guideline that offers a non-binding approach to the application of international law to cyberspace, yet its limited influence explains why more substantial frameworks are necessary (Schmitt, 2013). Lack of such structures means that future conflict is likely to degenerate, be misattributed, and undermine traditional humanitarian principles.

The Israel-Hezbollah War has a few more general insights into cyber warfare:

1. The application of cyber tools by Hezbollah resulted in strategic diversion, which demonstrates how a new organisation can create an inroad to states through military inferiority. Meanwhile, the cyber operations of Israel posed a question about the legal scope of actions of states in cyberspace
2. The use of cyber instruments to control perceptions was intentional on both sides, which revealed the psychological aspect of digital conflict.
3. The contemporary conflicts in the world have shifted to hybrid warfare, whereby traditional battles are no longer confined to being fought alone without the involvement of cyber and psychological realms. Cyber operations are the most efficient when they are used along with regular and irregular tactics, and their influence on the battlefield and perception is increased.
4. Regulatory and legal frameworks of cyberspace still do not keep up with the level of technological development. This gap is reflected in the Israel-Hezbollah conflict because it was involved in cyber activities without guidelines and accountability structures on international borders. This highlights the pressing necessity of the international agreement regarding the regulation of cyber warfare, such as the determination of what may be performed, the creation of norms of state conduct, and the protection of civilians against the effects of online attacks.

CONCLUSION

To sum up, the 2006 Israel-Hezbollah conflict was a pivotal point in the development of modern warfare since it proved how cyber operations may influence the psychological, informational, and strategic sides of a conflict. The war was one of the first to be fully hybrid as both sides distracted, intimidated, and influenced each other using digital means. As the case demonstrates, the tricks of the cyber strategy, including propaganda, disruption of communication, and manipulation of media, are also now a core part of the conflict, and they can modify perceptions and influence the consequences of the battle.

The war also supports the concepts of Realism: both a state, such as Israel, and a non-state organization as Hezbollah, operated cyber operations to achieve a strategic advantage, to survive, and to threaten the power of its opponent. Meanwhile, the war unveiled notable loopholes in international law since cyber-warfare is not clearly defined by the law and can hardly be controlled.

After all, the 2006 war teaches three lessons that remain: cyber warfare is now a strategic equaliser, the control of information is as vital as the control of the territory, and the wars in the future will be more and more mixed in conventional and digital forms. These lessons highlight the necessity to have stiffer international structures to oversee the increasing competition of cyber war in a globalised world.

REFERENCES

Al-Rizzo, H. (2013). Cyber warfare and hybrid conflicts in the Middle East: The case of the Israel–Hezbollah war. Middle East Security Studies Journal, 7(2), 45–62.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! Comparative Strategy, 12(2), 141–165. https://doi.org/10.1080/01495939308402915

Arreguín-Toft, I. (2001). How the weak win wars: A theory of asymmetric conflict. International Security, 26(1), 93–128. https://doi.org/10.1162/016228801753212868

Avital, L. (2007). The media battlefield: Hezbollah's propaganda in the 2006 war. Journal of International Communication, 13(1), 30–50.

Biddle, S., & Friedman, J. A. (2008). The 2006 Lebanon campaign and the future of warfare: Implications for army and defence policy. Strategic Studies Institute.

Carr, J. (2012). Inside cyber warfare (2nd ed.). O'Reilly Media.

Clarke, R. A., & Knake, R. K. (2010). Cyber war: The next threat to national security and what to do about it. HarperCollins.

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.

Deibert, R. (2013). Black code: Inside the battle for cyberspace. Signal Books.

Hoffman, F. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.

Kello, L. (2017). The virtual weapon and international order. Yale University Press.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Lobel, A. (2012). The propaganda war: Hezbollah's use of media during the 2006 Lebanon conflict. Middle East Policy, 19(2), 99–114.

Mearsheimer, J. J. (2001). The tragedy of great power politics. W. W. Norton.

Nye, J. S. (2010). Cyber power. Harvard Kennedy School Belfer Centre for Science and International Affairs.

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Rid, T. (2013). Cyber war will not take place. Oxford University Press.

Schmitt, M. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.

Shachtman, N. (2007). Hezbollah's cyber tactics in the 2006 war. Wired Magazine. Retrieved from https://www.wired.com

Tabansky, L., & Ben-Israel, I. (2015). Cybersecurity in Israel. Springer.

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.