

THE DIGITAL BATTLEFIELD: AI, DRONES, AND THE FUTURE OF WARFARE IN GAZA

Saqlain Ur Rehman¹, Abdul Samad², Dr. Irshad Ali Wassan³, Erum Naz⁴, Sabeen Azam⁵

¹Graduate Department of International Relations, Federal Urdu University of Arts, Sciences and Technology, Karachi

²Master's Department of International Relations, National Research Tomsk State University, Tomsk Oblast, Russia Federation

³Assistant Professor Department of Political Science, Shah Abdul Latif University, Khairpur, Pakistan

⁴Graduate Department of International Relations, Federal Urdu University of Arts, Sciences and Technology, Karachi Pakistan

⁵Lecturer International Relations, National University of Modern Languages, Karachi, Pakistan

¹saqlainurrehman0@gmail.com, ²absamad028@gmail.com, ³irshad.wassan@salu.edu.pk, ⁴erum0981@gmail.com, ⁵sabeen.azam@numl.edu.pk

DOI: <https://doi.org/10.5281/zenodo.15708996>

Keywords

AI Targeting Systems, Drone Warfare, Autonomous Weapons, International Humanitarian Law (IHL), Gaza Conflict, Ethical Warfare

Article History

Received on 13 May 2025

Accepted on 13 June 2025

Published on 21 June 2025

Copyright @Author

Corresponding Author: *

Saqlain Ur Rehman

Abstract

This study examines the transformative impact of artificial intelligence (AI) and drone technologies on modern warfare in Gaza, focusing on Israel's deployment of systems like "Lavender" for automated targeting and pervasive drone surveillance networks. It reveals that AI-driven tools enable rapid data analysis and precision strikes, enhancing military efficiency but at significant humanitarian costs. Lavender's algorithmic targeting—with a reported 10% error rate—and minimal human oversight blur distinctions between combatants and civilians, leading to disproportionate civilian casualties and psychological trauma. Continuous drone surveillance further exacerbates mental health crises among Gaza's population, particularly children. The integration of AI with cyber operations (e.g., disrupting communications pre-strike) and tunnel-mapping systems like Exodigo underscores emerging hybrid warfare tactics. Ethically, these technologies challenge adherence to international humanitarian law (IHL), especially principles of distinction, proportionality, and accountability due to algorithmic opacity. The analysis underscores an urgent need for robust legal frameworks, human oversight mandates, and ethical guidelines to govern autonomous weapons, emphasizing that technological supremacy must not compromise fundamental human rights in conflict zones.

INTRODUCTION

These are not the only changes in the way society changes and transforms under the influence of the digital environment that has dominated the range over the last 30 years and opened the door to a new era of war with absolutely new means to perform military activities. The beginning of the era of cyber warfare has probably been the most visible and

frequently mentioned factor of this paradigm shift recently (Rid, 2020). The possibilities with which the offensive cyber capabilities may assist military operations in the future are numerous. The use of these tools may at other moments be intended to supplement kinetic means a potentially more momentous change, both in terms of the domain of

military strategy and in the sphere of humanitarian protection is the great increase in the means available to directly affect adversary states without involving the employment of kinetic force in any way. Through the process of increasingly conventional military activity, cyber-competence could be used in a punitive manner, or a disruptive sense, as an aspect of what is now being lauded as so-called all-domains manoeuvre war, i.e., the establishment of decision advantage that exploits the cyberspace to afford operations in the Ground, Air, and Maritime Domains with the capability to deter and beat an opponent (Healey, 2013). These may involve sabotaging or disabling of guns of the opposing side by either tampering with them or through digital targets as introducing malware onto it, attacking destabilizing the computer systems of the opponent such as their ISR information systems or intelligence stores to derail the intelligence gathering efforts on their part or broadly on disrupting the digital build of the adversary in general like what could be seen in the armed conflict between Russia and Georgia in 2008 (Clarke & Knake, 2010).

A single real-life example worth mentioning in this regard would be the extensive cyber operations carried out by the U.S. and its allies who were fighting against ISIS, not just hacking the communication network and devices of the terrorist organization that was used to conduct propaganda campaigns and recruit new members but even interfering in the middle of drone attacks being constructed by the organization. Even more radical, possibly, is the possibility of applying offensive cyber capabilities and substituting the conventional military force, which is based on some form of kinetic energy. Part of such an operation could be initiated to reduce risks of major damage to the fixed adversarial facilities and, hence, reduce the possibilities of escalation.

A possible candidate of a cyber operation that had a deliberate, albeit secondary, physical effect is Operation Olympic Games or the Stuxnet malware released by the United States and Israel in a move against Iranian uranium enrichment activities in the Natanz facility and arguably far less devastating than the attempts by the militaries and intelligence agencies of the two countries to do the same using kinetic strikes delivered on fighter aircraft or

drones (Zetter, 2014). Meanwhile, we have observed during the last decade single cases of disruptive military cyber operations against the critical infrastructures of other states, say the country's electrical grid, or directly against civilian property with rather tremendous, most likely unintended impacts in an overwhelming number of states (Healey, 2013). These have been increasingly occurring and some could even be said to cautiously begin to overtake the attacking of more classic military targets and has resulted in a statement being made that with them the waging of conflict is creeping towards the coercion and control of civilian populations within adversary nations rather than an effort to destroy the opposing armed forces. Contemporary evaluations have also indicated the numerous dangers to both civilian individuals and properties, as undertaken by such operations. Considering the existing abilities and plans, it has been stated that as far as offensive military applications of cyber technologies in situations of conflict are concerned, the overall situation resembles that of air warfare in 1914; which means that more extensive operations with more advanced consequences can be expected in the next one to two decades (Rid, 2020).

Israel has a strong defence and offense system, while a locked country that has an enemy on all sides it covered all perspectives of defence and changed the concept of modern warfare. It increases military efficiency and minimizes human interventions. However devastating impact on humans and violates international human law (SETA, 2024). The most popular and active Artificial intelligence (AI) system in Israel is the Iron Dome which targets the short-range rockets. This AI reduces human intervention and also has rapid decisions without any threat (SETA, 2024). Israel also has a strong offense system which includes Habsora and lavender particularly it targets through identification. Another field where Israel developed its AI technologies is cyberattacks through defence and offense. AI-based cyberattacks can identify weaknesses in targeted systems and contain autonomous combat software exploiting those weaknesses. Israel has been deploying the majority of those AI systems in attacks against Palestine, especially after October 7, and minimizing human intervention in those processes, systems such

as Lavender overlook civilian-populated areas while identifying targets. (SETA, 2024).

1.1 Background Information

Evolution of digital technologies in modern warfare (AI, drones).

In recent years the news idea emerged among policymakers that AI technologies have the potential to change the character of war (Horowitz et al., 2018). The rapid advancement of new technologies like artificial intelligence (AI), drones, robotics, and other engineering technologies change warfare in unexpected ways.

However, new technologies expand the entry barrier, and maintaining a technological edge will be increasingly challenging (Scharre, 2019). In future conflict environments expanding dimension, converging domains and sensor proliferation, and increasing weapon range, speed, and autonomy. International security is threatened by the reactive advancement of hybrid warfare taking many forms including information operations, troop movement, cyber-attacks, and combinations of all these things (Murray & Mansoor, 2012).

It is believed that the current developments in technologies reliant on machine-learning algorithms (ML) and other such technologies narrowly defined as artificial intelligence (AI) today are due to enable the most fundamental changes in military operations both on the strategic and operational level as a part of the broader phenomenon of the future digital battlefield. There is no commonly agreed definition of AI in its broadest application but AI could be conceived as a constellation of processes and technologies that allow computers to supplement or substitute other specific tasks traditionally accomplished through humans, including decision-making and problem-solving (OECD, 2019). A common clean-cut described along these lines is that between AI representing a highly intelligent process with the ability to accomplish a large number of various tasks approaching those of a human mind, otherwise known as general AI as opposed to a narrow variety of the concept that would not only not exist but, indeed, may never have a chance to emerge even in the most optimistic projections, which goes by the term narrow AI (Russell & Norvig, 2021). Machine learning is a process, currently the

most common one of training algorithms, as a subcategory of narrow AI. Systems based on the technology are then trained using enormous volumes of data which then enables the system to create its model to produce some desired outcome i.e. to make predictions as opposed to working with the processing of hard-coded rules as had been the earlier conception of AI. This implies that the production is subject to various variant and interdependent variables including the model of the learning process and the resultant model but the resultant model is a function of the data that the algorithm is salted with. Among the natural qualities of this solution is the fact that a human operator can still see very little into the innermost technical functioning of the learning process and thus, at least to some extent, depending on the specifics of a particular situation and environment, the result of the operation becomes unpredictable (Gusterson, 2016).

The new period in drone warfare is described by the continuing proliferation of drone technology not only to new state and non-state actors but also across functional disciplines. Multiple fast-paced technological advances especially the arrival of AI enabled autonomy and translucency of the digital battleground. still, this drone technology is unfolding in a security terrain characterized by increased query and permeability, with new armament systems assuming their function as political logrolling chips, rather than military means. Drones, or remote-controlled upstanding systems, are far from a new technology. Drones are as old as aeronautics and air power itself. Austria used inflammatory balloons to attack Venice in 1849. The early 1900s saw balloons controlled from hence by introductory radio transmitters (Rogers, 2014). Both of these munitions can justifiably be appertained to as the first crude, independent upstanding systems. The forbears of Moment's fortified drones, similar to the US Kettering Bug, were developed during the First World War. But drones were no way directly used on the battleground until Israeli operations using loitering munitions in the 1980s. Drones had been stationed in warfare preliminarily, however. In the 1930s and 1940s, drones were suitable to collect intelligence due to remote radio regulators and abecedarian camera systems for upstanding

photography. Drone developments also accelerated during the Vietnam and Iran, Iraq Wars. The ultramodern drone period did not begin until the 1990s, despite before, frequent exemplifications of remote-controlled upstanding systems and their use of colours. This is substantial because detectors and communication systems progressed and became more dependable. The development of ultramodern drone technology can latterly be linked with three main time ages, or ages. In the 1990s through the 2010s, drones were substantially conceived of as advanced large airborne platforms. These enabled ongoing monitoring and targeted strikes. The first real-time transmission of videotape by the American Predator drone, stationed in Bosnia in 1994, consequently marks the morning of the First Drone Age. This was soon followed by the first drone strike during Operation Enduring Freedom in Afghanistan in 2001 (Bergen & Rothenberg, 2021). Drones of this period came in two Class III variants medium-altitude, long-abidance (manly), and high-altitude, long-abidance (HALE) drones. Both types carried either intelligence, surveillance, and surveillance (ISR) detectors or munitions. Drones therefore became enablers of remote warfare that allowed threat-antipathetic political leaders to avoid transferring “thrills on the ground” by fighting terrorism from hence. Those large drones were stationed in areas where the technologically superior side controlled the airspace and could fly large aircraft to overlook theatre-wide areas for extended ages of time. This increased the closeness of warfare. In addition to these large drones operated through space-grounded satellite links, military drone technology of the period also included lower vehicles. Class I drones, suggesting asset widgets, are an order that includes aircraft that can fly for 20 twinkles and fit in the win of one’s hand or small, hand-launched model airplanes used for original surveillance. Class II aircraft are mid-sized political drones with ranges that extend beyond the line of sight, importing between 150 kg - 600 kg. These drones bear a launch to be lifted into the air. Another type of airborne remote-controlled vehicle, kind of a cross between a drone and a bullet, has also given ground forces more precise strike capabilities than mortars or rockets. lollygagging munitions are designed to engage the target beyond

the line of sight with an explosive warhead that detonates on impact. These drones can stay loitering in the air for some time before striking their target and frequently feature high-resolution electro-optic and infrared cameras. maybe the most notorious loitering munition, the Israeli Harpy from the 1990s, proved effective in destroying radar installations and mobile bullet launchers. Vertical (new tech) and vertical proliferation (new actors) of drones define the Alternate Drone Age. For roughly thirty times, military drones were the exclusive tools of the most advanced fortified forces, with Israel and the United States as the first carriers in ultramodern service drone technology. still, the once two decades have witnessed the spread of drones into the hands of a wider array of lower-resourced countries, on-state regulars, and indeed terrorist groups. They’ve also been stationed to help transnational philanthropic operations (Gettinger, 2019). The global drone request has thus expanded thanks to the rise of new exporters, such as China, Iran, and Turkey. These proliferation dynamics have altered cost and threat computations about drone use in conflicts. Importantly, the exponential development of small and affordable consumer-grade drones in the early 2010s has accelerated these proliferation trends. marketable layman drone technology, together with the preface of smartphones that give fluently accessible control bias and detectors, has lowered the entry walls in terms of platform costs and supporting structure for penetrating air power means. This availability of technology has contributed to now exponential increases in drone fashion ability. Similarly, traditional air defences face difficulties fighting small marketable drones. Due to their material composition and flying mound, as well as multi-copter propulsion which makes them delicate to descry and block, these drone characteristics allow colourful military groups to “punch above their weight” (Singer, 2009). Drones have the eventuality to enable similar groups to beget military goods that are disproportionate to their limited coffers.

Statistics on drone usage and AI integration in Gaza conflicts

The Israeli military has used in its ongoing offensive in Gaza related to military planning and targeting. One is based on the persecution of mobile phones to

monitor the withdrawal of Palestinians from parts of Northern Gaza (Human Rights Watch [HRW], 2024). Another gospel calls for the army is to create a list of buildings or other structural targets to be attacked. Another thing the military calls - Lavender "indicates that the people of the Gaza Strip refer to them as belonging to a Palestinian group to describe them as military goals (Al Jazeera, 2024). The data included 10-year census data from the Gaza Strip, individual population data, information on civilian population movements, the presence of Israeli forces in Gaza, and the number of cumulative attacks in the 620 blocks of GazaFlick. The data also contained personal information. The surnames of the largest, most populous family members in each block (HRW, 2024).

Human Rights Watch analysed and mapped this data about Israeli military presence, responding to Israeli ideas in mid-November 2023, discovering that Israeli forces dominated most of North Gaza and had not yet entered Khan Yunis south. Human Rights Watch failed to reliably confirm the origin and use of information published online, but it resembles the data listed in media reports for planning military operations about evacuation surveillance systems. Evacuation monitoring systems are also based on other data sources (The Guardian, 2023). Human Rights Watch has notified the Data Protection Agency, Israel's Data Protection Agency of disclosure of this data (HRW, 2024).

Lavender:

Lavender is not an autonomous weapon but hastens the kill chain and makes killing increasingly more autonomous. AI targeting systems access and utilize data from computer sensors to evaluate what comprises a possible target statistically (HRW, 2024). Huge quantities of such data and analysis are collected by the Mossad and other intel agencies via surveillance of over 2 million Gazans. Owing to Lavender, the IDF marked thousands of Gazans as suspects for killing, deploying an AI-targeting recommendation system with scant human supervision and a non-restrictive casualty toll number (Al Jazeera, 2024).

Lavender has been (mis)used, often blurring the already nebulous lines between innocent civilians and Hamas operatives, all of whom have been

targeted en masse to deter future aggression." Lavender" traces and assesses people red-flagged as potential militants placing them on arbitrary kill lists (Al Jazeera, 2024). Lavender's ten percent error rate, caused in part by a rapid target corroboration process, is highly problematic and controversial. Lavender uses machine learning to assign residents of Gaza a numerical score relating to the suspected likelihood that a person is a member of an armed group. Based on reports, Israeli military officers are responsible for setting the threshold beyond which an individual can be marked as a target subject to attack (The Guardian, 2023).

Exodigo:

Exodigo a much less publicized underground mapping AI app scooped up \$105 million from venture capital and was founded by Israel Defence Forces (IDF) veterans and intelligence units. Exodigo departed from tradition by opting not to establish yet another cyber/digital company, as the majority of Israeli drone swarms, and army veterans do, but instead developed an Artificial Intelligence proprietary platform uniquely for underground mapping with multi-sensing tech developed through the simulation of multiple sensors, 3D visualization, and data merging which are all decisive in pinpointing underground Hamas tunnels (TechCrunch, 2023). Though Exodigo does not openly publicize this reality, this is its de facto intent and raison d'être.

Exodigo is highly expedient for Israel's specialist subterranean commando unit or the "Weasel" team who are aptly skilled in the logistical nightmare of subterranean combat (Haaretz, 2024). These elite underground Yahalom Units, trained for long drawn-out battles with Hamas in the 300 miles of labyrinthine tunnels Hamas purpose-built to hide and transport goods for military and strategic purposes (The Jerusalem Post, 2023).

1.2 Statement of the Problem

Artificial intelligence (AI) and drones used in Gaza have completely changed the balance of combat as they offer the possibility to target in less than a minute and with very little human input. Such systems as Lavender automatically label thousands of Gazans as military targets based on algorithm scores

of risks, causing mindless bombardment with an established ten percent error rate (Al Jazeera, 2024). Such automation is an ethical gray area because the control of the activity by humans is replaced with the decisions made by AI, which increases the risks to civilians, (attacks on settlements with large population density and failure to evacuate based on AI-tracked mobile data) (The Guardian, 2023). At the same time, these technologies question international humanitarian law (IHL), especially the concepts of distinction and proportionality due to the increased ambiguity of damage to civilians. Transparency in AI algorithms not being transparent as well as trusting such lethal decisions to the machine introduces a loophole in legal accountability, impeding the justice of violation and violating norms of warfare (SETA, 2024). This study aims to analyse tactical and ethical dimensions of AI/drone use in Gaza and to assess compliance with international humanitarian law.

2. Literature Review

2.1 Realism: AI/drones as force multipliers in asymmetric warfare.

Realism is basically divided into two categories namely classical realism (Thomas Hobbes, Thucydides, Niccol P Machiavelli) and neorealism (Kenneth Waltz and Mearsheimer). It is necessary to mention that another stream of realism appeared which has been strongly denied by the scholars representing realism called neo-classical realism (Gideon Rose, Norrin M. Ripsman, Jeffrey W. Taliaferro, Steven E. Lobell, and Fareed Zakaria). The classical realists concentrate on human nature as the chief cause of competition, the cause of war, the value of power, and intrastate issues. An example is Thucydides who believed that international conflict is fuelled by the conflict of ambition of the state based on the human propensity of pride and fear. Structural realism had it that the reason behind the competition amongst states, the balance of power, and the necessity to seek power is a survival activity of states and the international system was the father to all of this. All great powers of all types of regimes fall under the international system where incentives are put in place. Neorealism has two important strands namely; offensive and defensive. The defensive neorealists e.g. Kenneth Waltz 1983

contends that such constant quests of states perpetually acquiring power are mistaken and therefore states seek to acquire as much power as they can, such pursuits are foolish so they say. Offensive neorealists opposed this claiming that, more power is as needed as possible especially when in the right situation to seek hegemony (Mearsheimer, 2001). Concentration of the excessive force is a perfect tool for preserving the existence of states in the international system. The new stream of thought in realism that went against the fundamental assigned characteristics of realism (self-help, state-centric, and survival) is the neo-classical realism, which put forward a foreign policy theory taking into account the influence of factors within the borders and the presence of non-state actors in national and international policies (Ndzendze&Marwala, 2023). This strand of the traditional approach to security is deemed to be applicable in this study on the basis of implications of non-state entities active in the process of proliferation and applications of AI military technologies as part of the commercial sector and domestic politics. The advent of non-military problems after the Cold War like; environmental issues, health-related issues, migration issues, economic issues, and political issues gave birth to the most general plea of redefining the conventional form of the security approach by a queue of scholars dubbed as wideners. They reasoned that the agenda of security should include non-military issues by broadening security issues, referent objects, and securitizing actors of the security such that it includes the nonstate actors. According to Lin (2011), the increased threat of non-military threats and non-state actors, socioeconomic, cultural, and non-territorial threats on the immediate sunset of the Cold War imply that security has to be extended in terms of scope in order to accommodate the same. This approach towards security studies by the wideners is a term that is commonly used to define collectiveness by the various theories of the IR/security studies regarding incorporating nation-states and regional-local governments, international organizations, non-governmental organizations, press, and opinion of the people, and market, non-militaristic issues, and forces of nature into the security agenda cataclysms (Durak, 2024). The approach of prominent wideners

included: liberalism, peace theory, critical security studies, constructivism, human security, gender security (feminism), environmental security (green theory), and Copenhagen school that reflected on the aspect that nearly every international relations theory is made available under the umbrella or theoretic peculiarities of the sphere of security (Durak, 2024). Liberalism (John Locke and Immanuel Kant) examines the relationship of international politics based on mutual relations, cooperation, security, and peace. It acknowledges the role of both state and non-state players in the process of international security including; international organizations, non-governmental organizations, international conventions, and the endeavours of the transnational companies undertaken privately. Among the prominent classical liberal thinkers Friedrich August von Hayek promotes the idea of utilizing the power of the market to regulate the activities of people because the freedom of trade between the parties will reduce the chances of a conflict (Hayek, 1945). It is possible to argue that the multidimensionality of artificial intelligence (AI) can be proven both under the traditional and widens approach to international security but the scope of current research is limited to the military applications of AI, hence, the concept of traditional/realist form of international security will be drawn upon however the research has been informed by the general IR theoretical assumptions regarding international security.

2.2 Ethics of Autonomous Weapons: Moral responsibility and "killer robot" debates.

The fascination and terrorization of the manifold people by the possibilities of robotics and artificial intelligence to transform or possibly eradicate human existence on this Earth should be epitomized in the Terminator film series. Asking artificial intelligence with the name Skynet to rise against its engineers and humans to wage war to kill the human race. Even though it may be regarded that the entire screenplay of the Terminator movie is fiction and never going to take place, there is a strong scientific argument that artificial intelligence and the fast-growing robotics technology have raised a very intense debate just as to what may be the consequences of inventing new armaments that may

allow the robots to act freely in a war environment (Roff, 2014). In the ongoing debate on autonomous weapon systems there is one query, is the autonomous weapon system a mere continuation of all weapons developed since the fight of human beings or is it a revolutionary alteration of all weapons encountered thus far? Two underlying issues are in the discussion, the issues of law and the issues of ethics. In that sense, one may ask will conventional rules of the armed conflict, which have been elaborated in greater detail in the Geneva and Hague Conventions, still suffice to safeguard human rights in the age of robot wars? Is it also possible that these laws could have an acceptable legal framework to use autonomous weapons systems in the context of war in the future? (UNHRC, 2015). The other underlying question in the debate on autonomous weapon systems entails an ethical stand on the usage of such systems in armed conflicts shortly. Specifically, is it ethical in any way to delegate such an important life choice of killing another person to the machine? Given that, as far as we can tell, future applications of lethal autonomous weapons systems would be an abysmal ethical and legal violation. In this paper, the legal and moral bedside of the possible use of lethal autonomous weapons systems (LAWS) is going to be discussed.

In other terms, some definitions exist according to which the elaboration of a definition of a fully lethal autonomous weapons system (LAWS) is likely to be among the key challenges to elaborate an effective international response to the rise of ever more autonomous military technology, either regulation or development ban. The failure to agree that would be adopted unilaterally and could underlie a preventative moratorium on development was reflected in the inability of an international group of experts convened by the United Nations to develop a definition of autonomous weapons systems that would be adopted (or at least agreed) unilaterally. During this ambiguity, several stakeholders, including states, warring organizations, and scientists have been coming up with contrasting frames over the meaning they would define as LAWSs. The most widespread definition of LAWS is produced in a 2012 US Department of Defence (DOD) directive on autonomous weapon systems, which states that it is a weapon system that after being activated could

choose and shoot targets without additional intervention by a human operator. There are several definitions of lethal autonomous weapons systems which are based on the definition of the US Department of Defence. Some scholars believe, however, that this is an overly general definition. As an example, Roff has denied the use of the definition because the words select and engage have remote meanings that can be interpreted in different ways. Horowitz stressed the possibility of selecting a target, which had not been pre-selected by an operator. Crotoft has stressed the weapon's capacity to process information in making targeting decisions. Our effort to define LAWS will conclude with a couple more definitions so that we get a precise idea concerning this matter. The first definition that NGO Women International League of Peace and Freedom puts forward regarding Killer robots: they are entirely autonomous weapons systems. These are weapons that have no significant human control over their operation no decision can be taken about where and how to use them; against what or against when it is used; and the consequences of use.) The second definition was explained by scholars Austin Wyatt and Jai Galliot is "A fully autonomous Lethal Autonomous Weapon System (LAWS) is a weapon delivery system capable of making an active command decision whether to fire or not without human involvement in the loop of supervision or guidance." Deonna Neal who is a military ethicist is involved in this third definition, "She terms it as a robot that applies some type of artificial intelligence in its decision-making and can discriminate its targets and control how it can use force without the eyes of humans on target verifications or authorizations before killing someone." Based on these definitions, as one can identify, the basic term of LAWS is that of autonomy or independence in a judgment-free of human input on when and on whom to lay a deadly platform. Warner Sharkey cautions us that when we say the word autonomy of robots, then we should not confuse it with how it is stated in philosophy, politics, individual freedom, and everyday language. As such Sharkey categorized autonomous robots thus: scripted, scripted, where the robots follow a pre-scripted or plotted routine; supervised, where the robots have some planning, sensing, and monitoring capacity aided by the

human operators; and intelligent, which again is rather vaguely defined as being ones in which 'human intelligence' attributes are implemented in software to be used in the decision making, problem solving and information perception and interpretation. Nevertheless, Noorman and Johnson state that any of the above definitions of autonomy disregard our knowledge concerning the reality of technological development: there is much literature in science and technology studies (STS), that demonstrates that the technological development path is variable, multidirectional, and relies on internal processes of negotiations between various social groups (Women International League for Peace and Freedom, 2019). Nature or any other factor does not predetermine which technologies will be acquired and utilized and they cannot be predicted lending certainty. During development, as the technology is designed, it can evolve and transform owing to many variables such as an alteration in funding, a historical event, regulation, accidents, market signals, etc. The multiplicity of the conceptions of machine autonomy within the discourse of autonomous robots portrays the multitude of ideas, ambitions, and goals of the several groups within the society that are invested in the invention of such technologies."

2.3 Historical Context

2.3.1 Evolution of drone warfare

The US deploys drone warfare in carrying out counter-terrorism missions in Pakistan, Yemen, and Somalia, where many innocents have lost their lives and are heavily criticized. To give one example, in Pakistan, as of 31 Oct 2014, 416-957 civilians were killed by the 401 U.S. drone strikes carried out there since 2004 (Bergen et al., 2014). In a speech held at the National Defence University in 2013, President Barack Obama answered the criticisms against his policy of drone warfare claiming that it was actually a more humane application than other military options: It is true that conventional airpower or missiles are far less precise than drones, and are likely to cause far more civilian casualties and more local outrage, (Obama, 2013) he said. An Israeli military operation was also conducted in 2014 which included a heavy use of drone warfare conducted in the Gaza Strip known as Operation Protective Edge

that lasted between July 8 and August 26, 2014. Once again, heavy international criticism was on the level of civilian casualties. Of the above operation that was ostensibly to prevent the firing of rockets by Hamas against Israel, more than 2100 Palestinians died. On its part, Israel says that approximately 53 percent of them were civilians; the UN cited about 70 percent (UNHRC, 2015). A lot has been said about the attempts of Israel in trying not to kill civilians: the Israeli Foreign Ministry said that it had employed the most sophisticated weapons that are in the market today so that it can make sure that it only eliminates confirmed military targets and it reduces the number of collateral damages on civilians. Israel Defence Forces (IDF) stressed the significant contributions of drones in assisting the organization reduce civilian killings. About Israeli efforts the Chairman, of Joint Chiefs of Staff (CJCS), General Martin Dempsey, stated, as reported in the Jerusalem Post, that Israel had gone to extraordinary lengths to reduce potential collateral damage and minimize civilian casualties and that, the Pentagon had sent a lessons-learned team to go and work with the IDF to see just what they could learn out of the operation in Gaza, including its efforts to minimize the civilians, (Gross, 2014). A lot can be learned. A study of Operation Protective Edge as an illustration of the drone warfare fast emerging art can contribute to the clarification of the seemingly paradoxical issue of how dependence on drones could end up augmenting, instead of reducing, the number of civilians harmed (Kershner&Rudoren, 2014).

It is the intense surveillance measures done by the drones before the war that led to the subsequent collateral damage. The drones of Israel had taken years to develop their targets in Gaza, and in some instances neutralize before the drone attacks in Gaza killed 825 people between June 2006 to October 2011 according to the Palestinian Centre for Human Rights. During this time, in the course of Operation Cast Lead (December 27, 2008, to January 18, 2009), dozens were killed, and they may have included eighty-seven civilians, which testifies to the extent of drone activities that were occurring at that time over Gaza (Palestinian Centre of Human Rights, 2011). The long and widespread drone flights before military action were worth it in the sense that they offered targets. One senior commander on the blog

of the Israel Defence Forces says in the First UAV Squadron of the Israel Air Force (IAF) that We collect a lot of data then that eventually provides us with the capability to identify the targets that must be targeted. That is why when Operation Protective Edge started, the air force already had an extensive 'bank' of targets." These targets in a so-called bank became an enormous figure once the actual shooting war commenced on July 8, 2014. According to the IDF, it has hit 4,762 terror targets in the period of July 8-Aug 5, including 1,678 rocket launching facilities, 977 command and control centres, 237 military administration facilities, 191 weapons storage, and manufacturing facilities, 144 training and military compounds, and 1,535 additional terror sites.²⁶ Each of the 4,762 targets would again be hit multiple times and multiple times by multiple platforms. Moreover, the very definition of threat by Israel was such that a vast part of Gaza had become a targetable area: according to the report released in the New York Times on July 30, 44 percent of Gaza became a no-go area (Kershner&Rudoren, 2014).

2.4 Current Studies and Findings

As is observed in recent studies, artificial intelligence (AI) has an increasing capacity in warfare, and it is especially contested in Gaza strike missions. Lavender is an AI system that Israel has been accused of automating the "kill chain." Lavender crunches large volumes of data, such as census data, surveillance data, and metadata collected by personal devices, in order to statistically determine the probability of whether a person belongs to an armed group or not. It is said that the system flagged up to 37,000 people that should be specifically targeted and only the thin layer of humanity is being involved in control over these targeted strikes (Al Jazeera, 2024). Having an error rate of approximately 10%, and the possible correctness of thousands of civilians identified as someone else and thus killed or injured, proves the inaccuracy of AI in this hi-stake scenario (The Guardian, 2023).

Such automation of lethal decisions comes with ethical and legal questions, particularly regarding adherence to international humanitarian law. Human Rights Watch (2024) explains that Lavender using general statistical assumptions and lacking any significant human control breaks the distinction and

proportionality terms provided by the Geneva Conventions. Moreover, AI races and warfare experts warn that it is hard to hold anyone accountable because the nature of AI algorithms is unknown, especially when such technologies are employed in regions that are densely populated by civilians, such as Gaza (HRW, 2024).

At the same time, the psychological damage caused by the continuous drone oversight against the Gaza population has been measured in the humanitarian reports and NGO evaluations. The non-stop drone coverage has caused the development of a meaningful chronic level of psychological stress, especially in children, who complain of a lack of sleep, anxiety, and post-traumatic symptoms (HRW, 2024). Not only does the ubiquitous drone sound strike a fear of the imminent attack but it also provokes a loss of mental health as individuals are forced to feel that something or someone is watching over them all the time and in this case, the sky becomes a potent psychological warfare instrument.

Also, the more obscure AI platform Exodigo, founded by ex-leaders of the Israeli military, has pioneered new facets of digital warfare with the ability to chart out underground infrastructure. Multisensory data fusion enables the detection of Hamas tunnels that are being used logistically and as a fighting force, which has greatly boosted the underground capability of the Israel combat action (Haaretz, 2024). Although this is a militarily valuable capability, it raises more alarm bells about the scale of AI surveillance and targeting on the horizon.

Such discoveries emphasize the dual-use aspect of AI and drones since, on the one hand, they make the operations more accurate, and on the other hand, raise the risk to civilians in physical and psychological terms. These risks are also compounded by the absence of international regulation, and they set forth a particularly urgent necessity of implementing more ethical AI-enabled warfare systems, capable of global enforcement (SETA, 2024).

2.5 Gaps in the Literature

Although there is an increasing amount of research on AI and drone warfare, serious policy and scholarly disparities continue to exist. A significant weakness is that no significant analysis of the benefits of AI in

cyber warfare is conducted along with the use of drones. Although offensive cyber tools have been reported that aim to attack communication and surveillance systems (Clarke & Knake, 2010; Healey, 2013), little has been said about the coordinated means through which AI algorithms could be used to coordinate cyberattacks and kinetic attacks intended to cause maximum disruption in the strategic environment. This aspect of cyber-kinetic synergy has not been explored much, particularly in wars like Gaza where the AI system was used in the form of Lavender and the cyber platform at the same time (SETA, 2024).

Also, the information on the long-term traumatization of society and infrastructural denuding in AI-zoned regions is highly undocumented. Despite the fact that consequences of drone surveillance and aerial attacks on citizens have been revealed and emphasized by such organizations as Human Rights Watch (HRW, 2024), there is a lack of longitudinal research that would investigate the medium and long-term effects of these technologies on public health, cities, and infrastructure, educational systems, and economic reconstruction. The total harm caused by the constant AI-supported / supplemented warfare requires a significant prolonged scholarly and humanitarian investigation (The Guardian, 2023).

3. Findings

3.1 Case Study 1: AI-Powered Targeting Systems

The application of the Israel Defence Forces (IDF) in Gaza which uses AI-based targeting systems demonstrates an important change in contemporary warfare. An example is the usage of the AI system through what is known as "Lavender" in the escalation of 2023. Lavender used large databases (demographic files, communication meta-data, and social media patterns) and implemented machine learning algorithms to calculate the likelihood of people with respect to militant affiliations (Human Rights Watch [HRW], 2024). As it is reported, Lavender automatized the kill-chain decision process by ordering the airstrikes on thousands of people where little human intervention is involved (Al Jazeera, 2024).

The system is known to have had a 90 percent accuracy percentage but this means that there is a 10

percent margin for error and in such a populated area as Gaza, much civilian damage can occur (The Guardian, 2023). As an example, Lavender allowed strikes to take place within 20 seconds of authorization depending on patterns including SIM card sharing, and the approximate location of some of the suspected operatives, as opposed to actual militant behaviour (HRW, 2024). The critics state that this strategy causes indiscriminate targeting that blurs the borders between the combatants and the civilians.

The IDF justifies Lavender as a way of boosting the efficiency of its operations and limiting the exposure of soldiers in reference to the sudden secretive removal of hundreds of Hamas suspects. Nonetheless, the claimed accuracy is questioned because of independent evaluations. According to Human Rights Watch, a high number of targets were killed in their residences, sometimes in the presence of a family (HRW, 2024), which indicated the inability to observe the principle of proportionality under the rules of international humanitarian law.

The case highlights the dual-use issue of AI in war, where it gives a greater edge in tactical capacity but has the capacity to institutionalize systematic prejudices and accountability when mistakes happen. This increased the problem of making independent verification and recourse difficult and further made the ethical argument confusing regarding autonomous targeting systems because the algorithms are opaque, and no transparency is provided following the strike (SETA, 2024).

3.2 Case Study 2: Drone Surveillance Networks

The prolific operations of drone surveillance on Gaza, demonstrated by Israel, have thoroughly changed the art and science of intelligence and military tactics. Constant airborne monitoring possible due to drones and high-resolution cameras, as well as AI-based recognition algorithms, can ensure that the IDF always has eyes on Gaza and its urban environment (HRW, 2024). The obtained information is fed into targeting tools such as Lavender and assisted with the development of a flexible map of human activity, infrastructure, and possible militant activity.

Such close monitoring has had a great implication on the tactics of Hamas. It is reported that the group

has moved to deploying more tunnels underground and has diminished above-ground communication which points to a move towards the Israeli aerial superiority (Haaretz, 2024). Nonetheless, the surveillance blanket has also caused extensive psychological effects on the civilians of Gaza. Constant drone activity and sounds above, commonly referred to as a form of psychological warfare, have been attributed to the rise of anxieties, sleep, and long-term traumas, most of all in children (HRW, 2024).

There are ethical implications presented because of the very magnitude and permanence of this surveillance. As opposed to the conventional forms of reconnaissance, drone surveillance is an ongoing process, which makes it hard to distinguish between signals intelligence operations and bullying. Instilling the capacity to spy on the domestic activities of buildings or no-go zones without due process is a threat to privacy and the admissibility of the international law of human rights operated in occupied states (Al Jazeera, 2024).

Moreover, there is no explicit regulatory agenda that guides the storing, processing, and utilization of the amassed data. The personal information about more than 2 million Gazans that is potentially available in the hands of the IDF (phone metadata, facial recognition profiles, and patterns of behaviour) opens a vast database that may be used beyond the needs of the army (The Guardian, 2023). It has been suggested by humanitarian organizations to have increased transparency and accountability, with the most important being the relationship between security and the right to dignity and privacy.

3.3 Case Study 3: Cyber-AI Synergy in Warfare

Integration between AI and cyber operations was also observed in the 2023 Gaza conflict and became another frontier of hybrid war. Israel's military practices are highly increasingly the use of AI not just in kinetic targeting, but also arranged in conjunction with cyberattacks that halt communication and intelligence frameworks.

One such case is the reported usage of cyber-means to disconnect the mobile networks as well as the internet in Gaza several minutes before carrying out drone attacks. The strategic dispersion reduces the chances of the targets that may be able to run away

or communicate or record the assault. The use of AI further reduces this process by indicating where and when to communicate shutdowns would be effective on the aid of behavioural data and previously employed attack patterns (Clarke & Knake, 2010).

In this regard, Exodigo an Israeli AI system created by security technology startups reflects the dual-use character of cyber-AIs. Marketed to civilian underground mapping, Exodigo has played a pivotal purpose in locating and destroying the underground tunnels of Hamas. The militarization instinct is exemplified by such platforms: civilian AI systems can be easily militarized in order to advance military interests (Haaretz, 2024).

Nonetheless, this cyber-AI synergy presents serious legal and ethics-related challenges. The temporary switching off of services that are caused by cyberattacks interferes with the capability of civilians to access emergency services, humanitarian aid, and safety info. These measures can transcend the limits of international humanitarian law in case they are disproportionate to adversely impact non-combatants or strike against civilian infrastructure (UNHRC, 2015).

In addition, the lack of transparency in these cyber actions complicates the process of assigning accountability and determining the proportionate action. Accountability mechanisms do not keep abreast with the fast-changing digital battlefield without transparency. Similarly, cybersecurity enthusiasts and NGOs call on more transparent norms and increased oversight systems that would regulate the use of AI-accelerated cyber-implementation in the military arsenal (SETA, 2024).

3.4 International Involvement and Mediation

The increasing deployment of AI and autonomous systems into the war arena troubles the world and partially responds with regulation. The United Nations has tried a few times to discuss the ethics and the law requirement of lethal autonomous weapons systems (LAWS). Expert meetings to discuss the possible regulation or prohibition have been held in the UN Convention on Certain Conventional Weapons (CCW) since 2014. Nonetheless, controlling the use of water resources has not gained unanimous agreement because of the differing

national interests, particularly those of the biggest military powers (UNHRC, 2015).

The accountability gap has been filled by the non-governmental organizations (NGOs). A substantial number of civilian casualties and human rights abuses considered to be the result of the use of AI and drones in Gaza have been reported and documented by such organizations as Human Rights Watch and Amnesty International. Such groups promote the transparency of targeting procedures, the ethical regulations of AI algorithms, as well as the development of international legal standards by law regulating armed conflicts with the involvement of automated weapons (HRW, 2024).

These efforts notwithstanding the mechanisms of enforcement are very weak. The existing models of international humanitarian law cannot keep pace with the emergence and development of AI technologies thus exposing civilians to the threat of exposure in high-tech war zones.

3.5 Comparative Analysis

The Gaza war is one of the most drone-intensive battlefields in the world, and the one in Ukraine can be characterized by a greater role of AI in traditional military practice. Israel's deployment of AI systems such as Lavender and real-time aerial surveillance lasts in Gaza and targets specific steep cities, whereas it involves little ground troop presence (HRW, 2024). This focuses on the distant accuracy and eyes above perpetually with the result of a layer of surveillance and attack machinery.

In comparison, elements of AI including battlefield logistics, predictive maintenance, and drone swarm coordination have been incorporated by Ukraine. As part of the contemporary hybrid warfare in which troops face trench warfare tactics and cybersecurity challenges along with them (SETA, 2024), Ukrainian troops use Western technologies to endow AI capabilities that could be used to streamline decisions and optimize the use of resources (Ingraham, 2022).

Although both scenarios bring out the strategic benefit of AI, ethical issues are different. The absence of human control in the application of AI in Gaza alarms the safety and proportionality of the civilian front. In Ukraine, the problem is more on information integrity, cyber security, and fake news.

4. Conclusion

4.1 Summary of Key Findings

The application of artificial intelligence and drone technologies in Gaza has essentially revolutionized the mode of modern warfare providing a remarkable tactical advantage and causing graving humanitarian effects. Artificial Intelligence tools have allowed quick analysis of large amounts of data including census data, communication data, and movement patterns to locate probable targets faster than ever before minimizing the lives of the soldiers and utilizing proper resources by helping to find targets faster and spending less resources. Adding to this, 24-hour drone surveillance nets offer a constant battlefield picture that puts enemies on the back foot and allows airstrikes by pinpointing a target. These functionalities, however, are at a very heavy human cost. The fact that Lavender recorded an error rate of 10 percent and the strikes were authorized within 20 seconds of identifying their target has led to the collapse of the distinction between the combatants and the civilians thus leaving the highly populated locations to disproportionate effect. In addition to physical injuries, the constant drone surveillance has militarized the skies and long-term mental health trauma can be added to the list of drone war on humans, especially on children, as it creates anxiety, sleep disorder, and post-traumatic stress among them. More importantly, the lack of transparency in the process of algorithmic decision-making has undermined accountability, and it will become ever more challenging to hold any person or an organization accountable under International Humanitarian Law when they violate principles, like distinction or proportionality.

4.2 Implications for Future Policy

Gaza's experience dictates that there is a dire need for national and international policy revamping. The existing set of laws, such as the Geneva Conventions, is still insufficiently effective in managing autonomous targeting systems and algorithmic warfare and poses a real threat to human security. The United Nations Convention on Certain Conventional Weapons should focus on the development of legally binding agreements to outlaw fully autonomous military robots but insist on substantial human oversight of the given life-and-death decisions. At the same time, states are

supposed to establish effective systems to protect civilians, such as military AI system independent audits to check whether they operate in terms of international humanitarian law and identify algorithmic biases. Tough policies will need to be in place regarding civilian data collection and use, which is to ensure that mass surveillance is not abused, especially in occupied countries. What is more, ethical design standards to ensure explainable AI must be embraced to make the process of targeting less mystical and to make sure that the operation of lethal activities has to be dominated by human involvement?

4.3 Recommendations for Future Research

Future studies should prioritize AI's role in post-conflict reconstruction, examining its capacity to map infrastructural damage (e.g., via systems like Exodigo) while auditing algorithmic biases in resource allocation (TechCrunch, 2023). Crucially, interdisciplinary research must quantify long-term mental health impacts of AI-driven surveillance and strikes on Gaza's civilians, including generational trauma from constant drone monitoring and automated targeting (HRW, 2024). Additionally, legal scholars should investigate accountability frameworks for AI-enabled violations of international law, addressing gaps in attributing liability when autonomous systems cause civilian harm (UNHRC, 2015).

4.4 Final Thoughts

The state of the Gaza battle is the quintessence of the biological tussle between warfare innovation and ethical warfare. Although AI and drone technologies can provide tactical efficiency that has never been seen before, they will lead to a tendency of dehumanization being normalized by monetizing killing decisions that are abstracted using algorithms. The only way to ensure human dignity is preserved in this new era is by absolute adherence to three main factors: First, a precautionary policy that will have to dominate targets should always be verified by human judgment over algorithmic quickness, particularly in the area of civilians. Second, international collaboration is needed to enhance legal provisions to the effect that International Humanitarian Law develops accordingly with the

applications in autonomous weapons feature, where the emphasis is made on civil defence instead of military convenience. Third, moral leaders must be found in the technology developers and the military leadership that should refuse to develop systems that blind the responsibility and those that automate the use of violence where human control is lost. With war moving towards its algorithmic phase, the experiences of Gaza are being echoed around the world: without ethical fences tied to the irrefutable sacredness of human life, technological supremacy turns into a synonym for a moral defeat.

References

- Al Jazeera. (2024). *AI and Civilian Deaths in Gaza*.
- Al Jazeera. (2024). *AI Warfare and Civilian Harm*.
- Al Jazeera. (2024). Israel's AI-driven warfare: Inside "Lavender" targeting system. <https://www.aljazeera.com>
- Bergen, P., & Rothenberg, D. (2021). *Drone wars: Transforming conflict, law, and policy*. Cambridge University Press.
- Bergen, P., Sterman, D., & Schneider, E. (2014). *Drone wars: Transforming conflict, law, and policy*. New America Foundation. <https://www.newamerica.org/international-security/reports/drone-wars/>
- Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. HarperCollins.
- Gettinger, D. (2019). *Drone Databook*. Center for the Study of the Drone, Bard College.
- Gross, J. A. (2014). Pentagon sent team to learn from IDF Gaza operation. *The Times of Israel*. <https://www.timesofisrael.com/pentagon-sent-team-to-learn-from-idf-gaza-operation/>
- Gusterson, H. (2016). *Drone: Remote control warfare*. MIT Press.
- Haaretz. (2024). *Underground Warfare and Israeli AI Technologies*.
- Haaretz. (2024). Israeli AI company Exodigo quietly helping map Gaza's underground tunnel network. <https://www.haaretz.com>
- Hayek, F. A. (1945). *The Use of Knowledge in Society*. *The American Economic Review*.
- Healey, J. (Ed.). (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.
- Horowitz, M. C., Kahn, L., & Neuneck, G. (2018). *Artificial Intelligence and International Security*. International Committee of the Red Cross.
- Human Rights Watch (HRW). (2024). *AI, Targeting, and Psychological Effects in Gaza*.
- Human Rights Watch. (2024). Israel: Leaked Data Raises Serious Privacy and Targeting Concerns in Gaza. <https://www.hrw.org>
- Israel Defense Forces. (2014). *Intelligence in Operation Protective Edge*. <https://www.idf.il/en/minisites/operation-protective-edge/intelligence-in-operation-protective-edge/>
- Kershner, I., & Rudoren, J. (2014). Amid cries of war crimes, Israel insists its conduct is justified. *The New York Times*. <https://www.nytimes.com/2014/07/31/world/middleeast/amid-cries-of-war-crimes-israel-insists-its-conduct-is-justified.html>
- Lin, P. (2011). *Ethics and Autonomous Systems: A Widened Security Perspective*. *Journal of Military Ethics*.
- Mearsheimer, J. (2001). *The Tragedy of Great Power Politics*. New York: W. W. Norton.
- Murray, W., & Mansoor, P. R. (Eds.). (2012). *Hybrid warfare: Fighting complex opponents from the ancient world to the present*. Cambridge University Press.
- Ndzendze, B., & Marwala, T. (2023). *Artificial Intelligence and Emerging Power Rivalries in the Global Order*. Palgrave Macmillan.
- Obama, B. (2013). Remarks by the President at the National Defense University. The White House. <https://obamawhitehouse.archives.gov/the-press-office/2013/05/23/remarks-president-national-defense-university>
- OECD. (2019). *Recommendation of the Council on Artificial Intelligence*. Organisation for Economic Co-operation and Development.
- Palestinian Centre for Human Rights. (2011). *Annual report 2011*. <https://pchrgaza.org/en/annual-report-2011/>.
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

- Rogers, J. (2014). Drone warfare and the changing nature of armed conflict. *International Affairs*, 90(5), 1137–1146.
- Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
- Scharre, P. (2019). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.
- SETA Foundation for Political, Economic and Social Research. (2024). *Israel's use of AI in warfare: Violations of international law and impact on civilians* (SETA Report No. 260).
- SETA. (2024). *Israel's AI Military Strategies*.
- SETA. (2024). *Israel's Use of AI in Military Operations*.
- Singer, P. W. (2009). *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin Books.
- TechCrunch. (2023). *Exodigo: Mapping Tunnels with AI*.
- The Guardian. (2023). *Israel's AI Systems and Human Oversight in Gaza*.
- The Guardian. (2023). *AI-assisted warfare: Israel's use of algorithms in Gaza under scrutiny*. <https://www.theguardian.com>
- The Jerusalem Post. (2023). *Yahalom Unit: Inside Israel's elite tunnel warfare team*. <https://www.jpost.com>
- UNHRC. (2015). *Ethics and International Law in Autonomous Weapon Systems*.
- United Nations Human Rights Council (UNHRC). (2015). *Report of the detailed findings of the Independent Commission of Inquiry on the 2014 Gaza Conflict (A/HRC/29/CRP.4)*. <https://www.ohchr.org/en/hr-bodies/hrc/coi-gaza-conflict>
- Waltz, K. (1983). *Theory of International Politics*. Reading, MA: Addison-Wesley
- Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown.

