Arab American University
Faculty of Graduate Studies
Department of Legal Sciences
Master Program in
International Law and
Diplomacy

Israeli Methods of Cyber Espionage Against Civilians in the Occupied Palestinian Territory under International Law

Ahlam Ahmed Hassan Soboh
202112545

Supervision Committee:
Dr. Sania Abu Amro
Dr. Raed Abubadawia
Dr. Yakub Halabi

This Thesis Was Submitted in Partial
Fulfilment of the Requirements for the
Master Degree in International Law and Diplomacy

Palestine, 08/2025
© Arab American University. All rights reserved.

Arab American University
Faculty of Graduate Studies
Department of Legal Sciences
Master Program in International Law and Diplomacy

Thesis Approval

Israeli Methods of Cyber Espionage Against Civilians in the Occupied Palestinian Territory under International Law

Ahlam Ahmed Hassan Soboh
202112545

This thesis was defended successfully on 2.8.2025 and approved by:

Thesis Committee Members:

Name	Title	Signature
1. Dr. Sania Fisal Abu Amro	Supervisor	
2. Dr. Raed Mohammad Abubadawia	Internal Examiner	
3. Dr. Yakub Halabi	External Examiner	

Palestine, 8/2025

Declaration

I declare that, except where explicit reference is made to the contribution of others, this thesis is substantially my own work and has not been submitted for any other degree at the Arab American University or any other institution.

Student Name: Ahlam Ahmed Hassan Soboh

Student ID: 202112545

Signature:

Date of Submitting the Final Version of the Thesis: 12.5.2026

Dedication

To my resilient country Palestine, everything we do is for you.

To my beloved and supportive family.

To my husband without whom this achievement would not have been possible. We met within the walls of this university, where our shared journey began. Today, we finish what we started, side by side, and I could not have asked for a more inspiring, and loving companion throughout this journey and beyond.

To my beloved parents, who have been my first source of strength, love, and belonging. Your faith in me, your sacrifices, and your constant support have carried me through every stage of this journey. This achievement is as much yours as it is mine.

To my siblings, my lifelong companions and constant source of comfort. Your love, humor, encouragement, and presence have made every difficult stage lighter and every achievement more meaningful. I am grateful to have walked through life with you beside me.

Ahlam Ahmed Hassan Soboh

Acknowledgments

I would like to express my sincere gratitude to my supervisor, Dr. Sania Abu Amro, for her generous guidance, valuable insight, and continuous encouragement throughout the preparation of this thesis. Her support and academic direction were essential in helping me shape this research and complete it with clarity and confidence.

I am also grateful to the members of the examination committee for their time, review, and valuable comments, which contributed to strengthening this work. I extend my appreciation to the Faculty of Graduate Studies and the Department of Legal Studies at the Arab American University for providing the academic environment in which this research was developed.

This thesis also builds on the work of many scholars, researchers, journalists, human rights organizations, and legal experts who have examined the legal implications of cyber espionage, digital surveillance, privacy, data protection, artificial intelligence, and the use of emerging technologies in situations of occupation and armed conflict. Their work provided an important foundation for this study and helped make it possible to further examine Israeli cyber espionage practices against Palestinian civilians through the lens of international law.

Israeli Methods of Cyber Espionage Against Civilians in the Occupied Palestinian Territory under International Law

Ahlam Ahmed Hassan Soboh

Supervision Committee: Dr. Sania Fisal Abu Amro, Dr. Raed Mohammad Abubadawia and Dr. Yakub Halabi.

Abstract

This thesis studies the legality of Israeli cyber espionage methods that are used against civilians in the occupied Palestinian territory (oPt) under international law. Israel, which is a global leader in cyber technologies and an occupying state, has been using very modern technology to practice cyber espionage against a civilian population that is currently living under a prolonged military occupation. Israel's cyber espionage tools such as Pegasus Spyware, facial recognition technologies like Blue Wolf and Red Wolf, mass social media monitoring through profiling, surveillance UAVs, and AI tools like "Lavender", "The Gospel" and "Where's Daddy?" present serious legal concerns, especially as they have been intensifying after October 7, 2023.

The thesis assesses the legality of these practices using a descriptive analytical framework that incorporates both International Humanitarian Law (IHL) and International Human Rights Law (IHRL). The thesis concludes that Israel's cyber espionage practices in the West Bank violate key IHRL protections, including the rights to privacy, data protection, equality, dignity, and life, and amount to collective punishment under IHL. In Gaza, the use of AI-powered systems for targeted killings breaches core IHL principles of distinction, proportionality, and precaution, and further violates IHRL's protection of the right to life.

Therefore, this thesis adds onto the increasing legal study that is focusing on the new technologies being gradually used in different forms of armed conflicts, as it depicts these cyber espionage methods used by Israel as a kind of digital repression and unlawful targeting within an occupied setting.

Keywords: occupied Palestinian territory; cyber espionage; surveillance technologies; international humanitarian law; international human rights.

Table of Contents

Declaration ..... *i*
Dedication ..... *ii*
Acknowledgments ..... *iii*
Abstract iv
List of Definitions of Abbreviations ..... *viii*
Definitions of Key Terms and Concepts ..... *x*
Chapter One: Introductions 1
1.1 General Introduction 1
1.2 Statement of the Problem 2
1.3 Importance of the Study 3
1.4 Methodology 3
1.6 Scope of the Study 4
1.7 Literature Review 5
1.8 Thesis Outline 16
Chapter Two: A Historical Overview of the Legality of Espionage in International Law with Focus on Israeli Methods 18
2.1 The History of Espionage 18
2.1.1 Origins of Espionage 18
2.1.2 Espionage in Early International Legal Frameworks: A Historical Overview 22
2.2 Espionage in Wartime VS. Peacetime 23
2.2.1 Espionage in Wartime 23
2.2.2 Espionage in Peacetime 25
2.3 Intelligence Activities vs. Espionage 27
2.3.1 Definitions and Distinctions 27
2.3.2 Illustration from Israeli Intelligence 31
2.4 Israeli Traditional Espionage: Historical Context and Espionage Bodies 32
2.4.1 Early Pre-State Israeli Espionage Activities 33
2.4.2 Shin Bet (Shabak) 34
2.4.3 Aman 36
2.4.4 Mossad 37
Chapter Three: From Traditional to Cyber Espionage: Israel's Evolving Methods in the oPt 40
3.1 The Rise of Cyber Espionage and Israel's Emergence as a Cyber Power 40

3.1.1 Evolution of Cyber Espionage Technology 40

3.1.2 Israel's Strategic Shift to Cyber Espionage 43
3.2 The Israeli Cyber Espionage Uses in the West Bank 46
3.2.1 Tools and Deployment 46
3.2.2 Israeli Objectives from Cyber Espionage 54
3.3 The Israeli Cyber Espionage Uses in the Gaza Strip 55
3.3.1 Tools and Deployment 56
3.3.2 Israeli Objectives from Cyber Espionage 59
Chapter Four: Legal Analysis of Israeli Cyber Espionage Practices in the West Bank 62
4.1 Legal Context 62
4.1.1 The West Bank as Occupied Territory 62
4.1.2 Applicable International Legal Frameworks 64
4.2 Legal Assessment of the Israeli Uses of Cyber Espionage in the West Bank 68
4.2.1 Privacy and Data Protection 68
4.2.2 Freedom of Expression and Related Rights 74
4.2.3 Equality and Non-Discrimination 79
4.2.4 Collective Punishment 84
4.3 Legal Considerations Regarding the Use of Cyber Espionage Derived Information 88
4.4.1 Arrest and Detention Based on Digital Profiling 88
4.3.2 Coercion and Informant Recruitment 92
4.3.3 Targeted Killings and Lethal Operations 94
Chapter Five: Cyber Espionage and Military Targeting in Gaza 101
5.1 Legal Framework 101
5.1.1 Applicable Legal Frameworks in the Gaza Strip 101
5.1.2 Cyber Espionage as a Military Tool in Gaza 105
5.2 The Principle of Distinction: Cyber Espionage Generated Targets 107
5.2.1 Civilian vs. Combatant 108
5.2.2 Use of Predictive Surveillance and Profiling: Types of Cyber Espionage 111
5.2.3 Automation Bias or an Israeli Policy? Structural Failures in Distinction 117
5.3 Proportionality and Precaution in Cyber Espionage Enabled Attacks 121
5.3.1 Proportionality in Cyber Espionage Enabled Targeting 121
5.3.2 Precautions in Cyber Espionage Enabled Targeting 125
Chapter Six: Conclusion and Recommendations 131
6.1 Conclusion 131
6.2 Recommendation 135

References 138
الملخص 161

List of Definitions of Abbreviations

AI	Artificial Intelligence
CCTV	Closed-Circuit Television
CRC	Convention on the Rights of the Child
CERD	Committee on the Elimination of Racial Discrimination
CIA	Central Intelligence Agency
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
GCIV	Fourth Geneva Convention
GPS	Global Positioning System
HUMINT	Human Intelligence
IAC	International Armed Conflict
IAI	Israel Aerospace Industries
ICC	International Criminal Court
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
IHL	International Humanitarian Law
IHRL	International Human Rights Law
IMINT	Imagery Intelligence
ISR	Intelligence, Surveillance, and Reconnaissance
ML	Machine Learning
NIAC	Non-International Armed Conflict
NGO	Non-Governmental Organization
OECD	Organization for Economic Co-operation and Development
oPt	Occupied Palestinian Territory
OSINT	Open-Source Intelligence
SIGINT	Signals Intelligence
SMS	Short Message Service (used in communication surveillance contexts)
UAV	Unmanned Aerial Vehicle

UFED	Universal Forensic Extraction Device

Definitions of Key Terms and Concepts

Artificial Intelligence (AI):

Refers to computer systems that mimic characteristics of human intelligence, like learning, reasoning, and decision-making, with the aim of completing tasks without direct human intervention. In the context of this thesis, AI is used in surveillance systems, profiling, and automated military targeting.

Automated Decision-Making:

Refers to decisions made by algorithms or software systems without considerable human involvement. This could include identifying targets through metadata analysis or predictive models.

Cyber Espionage:

Refers to the covert exploitation of digital technologies and networks to get sensitive information, often for political, commercial, or military purposes, without the targeted entity's knowledge or approval

Cyberspace:

Refers to a dynamic, interconnected domain comprising digital networks, information systems, and the human users who interact with them. It encompasses the virtual environment where data is created, stored, transmitted, and manipulated, underpinned by physical infrastructures and governed by both technological protocols and human activities.

Espionage:

Refers to the gathering or attempting to gather information in territory controlled by an adverse party through an act undertaken on false pretenses or deliberately in a clandestine manner.

Facial Recognition Technology:

Refers to a biometric software application that uses AI to identify or verify individuals by analyzing their facial features.

Metadata:

Refers to data that provides information about other data, such as the time, location, sender, and recipient of a digital communication.

Machine Learning (ML):

Refers to a subfield of AI that allows computer systems to learn from data and improve performance over time without being explicitly programmed. When it comes to cyber espionage, ML is applied to improve surveillance.

Mass Surveillance:

Refers to the large-scale, blanket monitoring of a population's communications, movements, and behaviors by state or private actors. It typically involves the systematic collection of personal data without individualized suspicion or consent.

Open-Source Intelligence (OSINT):

Refers to the collection and analysis of information gathered from publicly available sources, such as media reports, social media, and internet content. It is a key method in both traditional and cyber espionage.

Profiling:

Refers to the systematic analysis of personal data to categorize individuals based on perceived behavioral patterns, characteristics, or potential risks.

Signals Intelligence (SIGINT):

Refers to the interception and analysis of electronic signals and communications for intelligence purposes. It includes monitoring phone calls, internet activity, and other forms of digital communication, often by military or intelligence units.

Targeted Killing:

Refers to the intentional and pre-meditated use of lethal force, by a State or organized armed group against a specific individual outside their physical custody.

Chapter One: Introductions

1.1 General Introduction

"Knowledge of subject races or 'Orientals' is what makes their management easy and profitable; knowledge gives power, more power requires more knowledge, and so on in an increasingly profitable dialectic of information and control." Said, E. W. (1978). Orientalism (p. 36). New York: Pantheon Books.

The link between knowledge and control, that Edward Said explains in his book within the context of colonialism and colonial power, is still important and even much more relevant within the increasingly evolving digital age. For example, espionage, which includes covert intelligence gathering and various forms of mass surveillance, has historically been used to have more control. What has changed, however, is the technological advancements with which such control is now exercised. In the twenty-first century, espionage has evolved beyond physical means, becoming multinational, data-driven, and typically completely invisible. Thus, states can infiltrate private data, collect sensitive information typically under the disguise of security and counterterrorism. This change creates complicated legal implications, especially when cyber espionage is used in asymmetrical power circumstances like military occupation.

This global change in espionage has become more evident in circumstances of prolonged military occupation and systemic inequity. Thus, this dynamic of such digital practices is clearly illustrated in Israel's use of cyber espionage methods. Historically, Israel has been using espionage methods to gain intel on Palestinians since the beginning of its occupation. Currently, as an occupying power and as a lead producer and exporter of espionage and surveillance technologies, Israel has been using its cutting-edge technologies extensively and systematically against occupied Palestinians. With technologies like spyware, facial recognition systems, social media monitoring, unmanned drones, AI profiling tools like the Lavandar project recently used in Gaza, Israel has been monitoring the everyday life of millions of Palestinians under their occupation.

The consistency of cyber espionage with international law remains a controversial topic. Traditional scholars argue that since international law does not explicitly prohibit cyber espionage, then its practices remain legality ambiguous, and cannot be definitively prohibited. Meanwhile, growing voices within the legal field have been arguing that cyber espionage does

in fact violate key principles of international law, whether principles of public international law, such as territorial sovereignty and non-intervention, or principles of international human rights and humanitarian law.

The urgency of this legal debate in the specific context of the Israeli occupation, has become more vivid in the aftermath of the resumption of hostilities in Gaza on October 7, 2023. Since that date, Israel has triggered an unprecedented scale of military operations in the Gaza Strip, in addition to an unprecedented level of violence in the West Bank. Therefore, Israel has been intensifying its use of cyber technologies under the loose claim of counterterrorism. Technologies such as the dependence on AI-driven profiling, mass metadata analysis, and more in-depth social media tracking have significantly increased. Israel has been using these technologies to justify different kinds of action including detention, suppression of political expression and even targeted killings. Similar to the Gaza bombings, this digital domination is presented as a component of a larger war on terror; however, in reality, it frequently targets civilians who have no connection to armed groups, which raises significant legal concerns under international law.

Therefore, this thesis aims to investigate the legality of Israel's cyber espionage methods against Palestinians in the occupied Palestinian territory (oPt). It begins by providing a historical overview of espionage under international law, in addition to an overview of Israel's historical espionage methods. It then provides a clear understanding of the emergence of technologies and cyberspace that presented more legal challenges to addressing cyber espionage. It focuses on the emergence of Israel as a cyber power and how it began using such methods against Palestinians and even beyond. The thesis also aims to provide a clear distinction between the legal framework governing the West Bank and those governing the Gaza Strip. Therefore, it provides in-depth legal analysis under both International Human Rights Law (IHRL), and International Humanitarian Law (IHL).

1.2 Statement of the Problem

Due to the drastic increase in the use of cyberspace by governments to collect certain information about civilians, many debates have been surfacing regarding the legality of such acts. Israel, being the occupying power in the oPt, has been using several methods to collect information on Palestinian civilians, including the use of Pegasus spyware, the facial recognition systems, the mass surveillance of Palestinians on social media, surveillance UAVs, AI-driven profiling such as the Lavender project, The Gospel, and Where's Daddy? However,

due to the lack of clear regulations addressing cybersecurity in international law, the question of the legality of such uses under both IHL and IHRL remains a controversial topic that needs further investigation.

1.3 Importance of the Study

As the use of several methods of cyber espionage has been increasing with further ongoing technological advancement, it has become more crucial to determine the legal scope of such uses. In the context of the Israeli occupation, determining the legality of Israel's cyber espionage methods has become increasingly necessary after their extreme use in the aftermath of October 7, 2023. Thus, the importance of the study lies in the need to fill the gap in the available literature, though offering a context-specific legal classification of Israeli cyber espionage practices.

1.4 Methodology

This thesis uses a descriptive analytical research approach, that is based on legal methodology, to evaluate Israel's cyber espionage tools and methods in the oPt and assess their compliance with applicable international law standards. Thus, the study is based on a variety of both primary and secondary sources, including international treaties, customary law, UN resolutions, UN reports, reports from human rights organizations, state practice, legal academia, and confirmed media investigations.

The legal analysis involves applying applicable sections of both IHL and IHRL to the documented practices, focusing particularly on fundamental concepts such as the right to privacy, equality, protection of minors, prohibition of collective punishment, as well as principles of distinction, proportionality, and precautions. Therefore, this allows a context-specific analysis of whether Israel's use of cyber espionage in both the West Bank and Gaza adheres to or violates established legal norms.

1.5 Research Questions

Main Research Question:

To what extent do Israel's cyber espionage practices targeting Palestinian civilians in the occupied Palestinian territory (oPt) comply with international law?

Sub-Questions:

1. Questions Related to the Historical Foundations of Espionage

- What is espionage, and how has international law dealt with it throughout history?
- What is the difference between espionage and intelligence gathering?
- How does international law treat espionage during wartime and during times of peace?

2. Questions Related specifically to the Israeli Practices

- How has Israel historically employed espionage against Palestinians in the oPt?
- What is cyber espionage, and how has Israel emerged as a global cyber power?
- What cyber espionage tools and methods has Israel used against Palestinian civilians in the West Bank and in the Gaza Strip?
- What are the intended objectives of Israel's cyber espionage practices in the West Bank and Gaza Strip?
- How do these practices differ between the West Bank and Gaza in both application and context?

3. Questions related to the Legal Frameworks

- What legal frameworks apply to the West Bank and to the Gaza Strip, especially when looking at Israel's cyber espionage practices?
- Which principles of international law, especially IHRL and IHL, govern the conduct of an occupying power in relation to cyber espionage?

4. Questions Related to the Legal Assessment

- Do Israel's cyber espionage methods violate the right to privacy under IHRL?
- Do Israel's cyber espionage methods violate the right to freedom of expression, equality and non-discrimination?
- Can Israel's cyber espionage methods be seen as collective punishment under the law of occupation?
- Do Israel's cyber espionage methods violate fundamental principles of distinction, proportionality, or precautions in attacks under IHL?

1.6 Scope of the Study

This thesis is limited in scope to the following dimensions:

- **Legal Scope:** The research scope is limited to certain branches of International Law which are IHL and IHRL, because they directly relate to the conduct of an occupying power and the rights of civilians.

- **Geographical Scope:** The thesis is limited to a certain geographic area which is the oPt (the West Bank, including East Jerusalem, and the Gaza Strip).
- **Temporal Scope:** There is no particular temporal scope for this research. The thesis gives attention to developments in Israeli cyber espionage methods throughout history leading up to October 7, 2023, and its aftermath while highlighting relevant historical context as needed.

1.7 Literature Review

There are numerous studies published that discuss the essence of espionage in general, and cyber espionage specifically. There are many papers that discuss the foundational legal debates related to cyber espionage through clarifying the definition of cyber espionage, the challenges in regulating it, and analyzing which legal principles apply to it.

For instance, Ella Shoshan's thesis titled "Applicability of International Law on Cyber Espionage Intrusions," published in 2014, studies the relationship between cyber espionage in peacetime and public international law, focusing on incursions by the state into digital data that is under the authority of another state. After clearly distinguishing between cyber espionage and other cyber intrusions, such as cyberattacks, Shoshan practical issues with traceability and regulation, pointing out how cyberspace anonymity impedes legal responsibility. In her legal analysis, Shoshan investigates whether customary international law forbids espionage in general and cyber espionage in particular. She concludes that neither *opinio juris* nor consistent governmental practice are adequate to create a definite ban. To determine whether cyber espionage is legal the author instead looks to concepts like sovereignty, non-intervention, and territorial jurisdiction. She contends that a state may violate its sovereignty and authority if another state gains unauthorized access to its protected data, which is kept on servers located on its territory. [1]

After that, the thesis refutes popular claims that cyber espionage is permissible under the idea of anticipatory or self-defense, contending that these claims are not applicable in peacetime until there is an immediate threat of armed conflict. Shoshan highlights the Tallinn Manual and other attempts to apply international law to cyberspace in a similar manner, concluding that fundamental ideas like sovereignty and non-intervention are still applicable and ought to be upheld in digital settings. Although espionage is not expressly forbidden by international law,

[1] Shoshan, E. (2015). Applicability of international law on cyber espionage intrusions.

the thesis concludes that state-sponsored cyber espionage intruders into another state's protected data are legally challenging, mainly because they violate the target state's sovereignty and jurisdictional rights. Shoshan contends that the lack of a particular treaty or customary rule does not make such actions legal; rather, their inconsistency with fundamental international legal principles makes them unlawful and requires oversight.[2]

Similarly, Christopher S. Yoo in "Cyber Espionage or Cyber War?: International Law, Domestic Law, and Self-Protective Measures", published in 2015 analyzes if cyber espionage, including surveillance and data interruption could be considered under international law that govern armed conflict. Yoo uses several examples to investigate, such as the NSA surveillance programs. She uses the examples to study the applicability of *jus ad bellum* and *jus in bello* on cyber activities. Yoo discusses that most of the cyber espionage does not meet the legal requirements necessary to qualify as an "armed attack" or to activate the Geneva Conventions' or the law of armed conflict. He specifically argues that cyber activities do not qualify as use of force as entitled in Article 2(4) of the UN Charter, nor does it trigger self-defense rights that are enlisted in Article 51 of the Charter. Similarly, he argues that cyber-attacks typically fall short of meeting the requirements to qualify as an international or non-international armed conflict under the law of armed conflict. Yoo's main findings in the paper illustrate that tools used for cyber espionage remain a legal dilemma, since they breach territorial sovereignty, but they are not properly addressed in international law. His main conclusion is that cyber espionage is mostly unregulated by current international legal frameworks. He emphasizes that this disparity sheds light on the urgency of strengthening technical defenses in the meantime while also highlighting the need for new legal standards tailored to the cyber world.[3]

Moreover, Russell Buchan in "The International Legal Regulation of State-Sponsored Cyber Espionage", published in 2016, examines if state sponsored cyber espionage methods are prohibited or controlled under principles of international law. Buchan initially starts by clearly defining cyber espionage as the unauthorized and frequently clandestine gathering of private data via the internet, usually by state actors. He explores several methods of cyber espionage, such as China's Unit 61398 and the NSA's global surveillance programs. Buchan argues that since there are no clear treaties or principles in international law that regulates the use of

[2] *Ibid.*

[3] Yoo, C. S. (2015). Cyber espionage or cyberwar?: International law, domestic law, and self-protective measures. Cyberwar: Law and Ethics for Virtual Conflicts (Jens David Ohlin, Kevin Govern, Claire Finkelstein, eds., 2015), U of Penn Law School, Public Law Research Paper, (15-3).

cyberspace, assessing the legality of cyber espionage must be in accordance with general principles of international law, particularly, territorial sovereignty and non-intervention. In terms of territorial sovereignty, Buchan argues that even in the absence of physical harm, a state violates the principle of territorial sovereignty when it participates in cyber espionage by invading cyber infrastructure that is physically situated within another state's territory. [4]

In terms of non-intervention, Buchan argues that in situations where a state's private data is sent or held via servers or infrastructure in other countries, information appropriation may amount to a coercive intervention in a state's internal affairs, even if territorial sovereignty is not directly involved. This is particularly true when it targets delicate diplomatic or governmental responsibilities. Buchan's main findings in the paper are that even though cyber espionage is not explicitly banned in international law, it can be considered unlawful when it violates key principles of public international law such as territorial sovereignty and non-intervention. He thus portrays cyber espionage as a developing field where established values like sovereignty and non-intervention continue to impose significant legal limits.[5]

Such literature that focuses on the legal debates around the topic cyber espionage provides a significant theoretical framework. However, they preview cyber espionage as only between sovereign states and treat it as a legal grey zone. Therefore, they rarely delve into the use of cyber espionage methods against civilians, specifically in the context of occupation. This thesis fills that specific literature gap through clearly analyzing the applicability of international law principles on cyber espionage methods in an underexplored context, which is the Israeli occupation of the Palestinian territory. It examines both international humanitarian law and international human rights law, as it distinguishes between the legal rules governing Gaza and the West Bank.

Other scholars have tackled a specific form of cyber espionage from a human rights law perspective, which is mass surveillance. For instance, Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi and Amandine Scherrer in "Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law", published in 2013, commissioned by the European Parliament after the 'Snowden' disclosures, provides thorough political and legal analysis of mass surveillance initiatives by five European Union (EU) nations: the Netherlands, Germany, Sweden, France, and the United

[4] Buchan, R. J. (2016). The international legal regulation of cyber espionage. Tallinn Papers, 65-86.
[5] *Ibid*.

Kingdom. The authors make the case that these surveillance activities represent a major change from conventional, focused intelligence collection to the widespread, indiscriminate, technologically facilitated mass interception of digital communications, including metadata and content, frequently carried out with little to no oversight. [6]

The paper frames this kind of surveillance as a serious democratic dilemma that jeopardizes European rule of law, transparency, and collective liberties, rather than just as a conflict between data protection and national security. The researchers outline how these countries participate in international data-sharing networks. The scholars notably discuss the legal foundations controlling these actions, and how they are seen as vague, containing flaws and inadequate supervision mechanisms. Although intelligence operations are frequently regarded as national responsibilities, the authors argue that the EU does have the legal and political power to step in, particularly when surveillance methods violate the EU Charter of Fundamental Rights and jeopardize internal security, individual privacy rights, and trust among EU institutions. Regarding this, the authors suggest more judicial and parliamentary monitoring, regulation of intelligence sharing at the EU level, and the establishment of guidelines that mark the limits of lawful surveillance.[7]

The scholars stress the risk of normalization, in which widespread surveillance is made to seem acceptable in democracies through the use of technology, secrecy, and counterterrorism rhetoric. Thus, the scholars' findings are that the mass surveillance operations of the United States are frequently mirrored, enhanced, or made possible by the surveillance programs of EU member states, and that these practices are generally incompatible with EU legislation and democratic ideals. In order to protect civil rights and keep monitoring from becoming an unchecked, systemic threat to democracy, it urges immediate reform and oversight procedures at the national and EU levels.[8]

Similarly, Monika Zalnieriute in "An International Constitutional Moment for Data Privacy in the Times of Mass Surveillance," published in 2015, analyzes the question of whether the right to privacy developed from a binding norm to customary international law, specifically in the context of mass surveillance tools. The author makes a distinction between the more specialized

[6] Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F., & Scherrer, A. (2013). Mass surveillance of personal data by EU member states and its compatibility with EU law. Liberty and Security in Europe Papers, (61).
[7] *Ibid*.
[8] *Ibid.*

concept of data privacy, which entails control over the processing of personal digital data, and the more basic right to privacy, which has long been recognized under human rights law. The paper examines various theoretical approaches to customary international law to determine if data privacy has formed into legal responsibility under international law. [9]

Zalnieriute asserts that modernist theories, which place more emphasis on broad agreement and normative urgency, support the notion that the scope and visibility of mass surveillance have sped up the evolution of international legal norms, while traditionalist views may question data privacy's status as customary international law due to fragmented state practice. The author then traces the different interpretations of Article 17 of the ICCPR and 8 of the ECHR, to cover data privacy. However, the paper also notes that the scope of existing frameworks is limited by the absence of a global treaty, the variety of national data privacy laws, and the lack of effective enforcement mechanisms. accepted as a standard of customary international law have been established by the extraordinary worldwide outcry against extraterritorial mass surveillance, technological advancements, and growing legal activism. Zalnieriute is a major advocate of modernism, arguing that even in the absence of a formal treaty, the legal system is already changing to perceive data privacy as an international duty. [10]

In addition, Eliza Watt in "The Right to Privacy and the Future of Mass Surveillance", published in 2017, offers a normative and legal analysis of widespread cyber surveillance initiatives, focusing on those utilized by the United States and the United Kingdom. The paper highlights certain tools that work on collecting digital communications from millions of people, usually without individualized suspicions and warrants to do so. Watt highlights that the United States and the United Kingdom adopt a double standard—their domestic laws grant citizens more legal protections than foreigners, thereby disregarding non-nationals from privacy safeguards—the paper shows that both practices are discriminatory. Therefore, this directly violated IHRL's non-discrimination principle, and more specifically Articles 17 and 2 of the International Covenant on Civil and Political Rights (ICCPR), in addition to Article 8 of the European Convention on Human Rights (ECHR). [11]

[9] Zalnieriute, M. (2015). An international constitutional moment for data privacy in the times of mass-surveillance. International Journal of Law and Information Technology, 23(2), 99-133.
[10] *Ibid.*
[11] Watt, E. (2017). The right to privacy and the future of mass surveillance. The International Journal of Human Rights, 21(7), 773-799.

Thus, importantly, the researcher argues that the beyond territorial reach of these treaties does require states to protect privacy rights even when dealing with people outside of their borders. In addition, she also argues that the legal opinions of nations such as the United States, which maintain that their duties do not extend beyond their borders, are in fact incompatible with international law. Moreover, Watt also explains that foreign mass surveillance is an unjustifiable violation of the right to privacy that is deeply protected under international law. Watt argues that PRISM, Tempora, and similar programs do not satisfy the criteria of lawfulness, need, proportionality, or legitimate objective after reviewing legal frameworks and standards established by international law. These technologies, which lack effective control, judicial review, or protections, amount to indiscriminate data collecting even if they are presented as counterterrorism tools. For example, they are predicated on domestic rules that are too general and do not specify who can be targeted, for what duration, or for what reasons. Importantly, both Article 17 ICCPR and Article 8(2) ECHR require states also in their surveillance methods to be very strictly required, for it to be reasonable, and based on easily accessible domestic legal frameworks. [12]

Therefore, the paper highlights that, even in cases when communications are not actually used, their possible access already amounts to a violation of privacy under IHRL. Thus, Watt suggests that the Council of Europe's legally binding multilateral agreement known as the "Intelligence Codex" should be adopted to address these issues. That is because it would require court orders to have access to the public's communications, it would forbid mass surveillance, and forbid espionage between friendly states. Therefore, Watt's main finding in her paper is that mass surveillance initiatives such as Tempora and PRISM are incompatible with the current IHRL framework. She argues that to counter the growing challenges that are increasingly being posed by unrestrained cyber espionage, especially against foreign people, she advocates for stricter legal regulation. [13]

The available literature that focuses on mass surveillance and its legality under international law, is mainly focused on state conduct in western states, and does not situate such practices in the context of an occupation. This thesis fills this gap through applying international law interpretations on cyber espionage, particularly in the case of Israel's cyber espionage methods against the Palestinian people they occupy. In addition, it does not only do so through the lens

[12] *Ibid*.
[13] *Ibid.*

of International Human Rights Law, but also through the lens of International Humanitarian Law.

Furthermore, other literature focusses specifically on Israeli cyber espionage methods in the oPt, and beyond. For instance, Benjamin G. Waters in "An International Right to Privacy: Israeli Intelligence Collection in the Occupied Palestinian Territories", published in 2016, investigates Israeli surveillance practices in the occupied Palestinian territory, particularly Unit 8200. As Israel's military signals intelligence unit, Unit 8200, was revealed to be conducting mass surveillance on Palestinian civilians and gathering very personal type of information such as sexual orientation, with the purpose of using them to coerce the Palestinian civilians to become informants. [14]

Waers analyzes this Israeli practice through the lens of IHRL, particularly the International Covenant on Civil and Political Rights (ICCPR), and IHL. Using the Vienna Convention on the Law of Treaties, ICJ case law (such as the Wall case), and General Comment 31, he first refutes Israel's argument that the ICCPR does not apply extraterritorially. He contends that the ICCPR does, in fact, bind Israel's actions in the oPt. He then delves into Article 17 of the ICCPR which guards arbitrary or illegal invasions of privacy, particularly because they disproportionately target civilians without ties to security threats. Waters then analyze IHL, particularly the Hague Regulations and Geneva Convention IV, to highlight that occupying powers are obligated to safeguard protected individuals' civil rights, including their right to privacy. Therefore, Water's key finding is that the Israeli mass surveillance of Palestinians in the oPt marks a violation of IHRL and the laws of occupation in IHL.[15]

Elia Zureik in "Strategies of Surveillance: The Israeli Gaze", published in 2016, provides a comprehensive examination of Israeli surveillance, particularly against Palestinians, while focusing on the themes of colonial control, excessive power and discrimination. Zureik focuses on how Israeli surveillance is used to force domination over Palestinians through population management. Therefore, Israel is using surveillance as a security tool, in addition to an instrument of colonial control. Zureik argues that this control through the Israeli surveillance practices is a part of the larger legal, psychological, technological and spatial control imposed by Israel. In his paper, Zureik also highlights that Israeli surveillance is a colonial tradition that

[14] WATERS, B. G. (2016). An International Right To Privacy: Israeli Intelligence Collection In The Occupied Palestinian Territories. CAP. UL REV, 677, 2.
[15] *Ibid*.

dates back to the British Mandate. The techniques used by Israel, such as the permit system, fingerprints, and identity documentation, have been used in other colonial settings, and have since been enhanced by Israel. Zureik also importantly underscores that surveillance can be seen as a form of racialized domination. Surveillance techniques utilized by Israel are not equally being used across the population, as it is being disproportionately and violently directed at Palestinians specifically. Therefore, it is based on categorizing Palestinians as threats. The study also examines the human aspect of surveillance, pointing out the dependence on networks of cooperators and informants. Such individuals are frequently threatened with extortion, denied permits, or offered financial incentives in exchange for giving intelligence about other Palestinians. Zureik argues that technical surveillance, such as the use of biometric technologies, predictive profiling, and metadata collection, is used in conjunction with this human information gathering. Furthermore, Zureik explores how these Israeli surveillance techniques can then be applied to other populations, not just Palestinians. Thus, Zureik offers a comprehensive explanation of how surveillance in the oPt a security issue is not just but also a key component of a larger colonial endeavor that combines ideology, technology, and the law to subjugate an occupied people.[16]

Likewise, Ronit Lentin in "Race and surveillance in the settler colony: the case of Israeli rule over Palestine", published in 2017, argues how Israel has formed its state through making its surveillance practices, racialized control, and militarized governance a crucial part of its structure. Therefore, Lentin emphasizes that Israel's surveillance is fundamental to its colonial project, as its purpose is not merely a security measure, but also a main tool for both racial and colonial domination. Similar to Zureik's paper, Lentin highlights how Israel's technological control, such as data manipulation, permit systems, biometric ID cards, and social media surveillance, is all a form of racialized monitoring. [17]

Notably, Lentin's article also discusses that Israel's cyber surveillance tools have been specifically used for repression. An example she provided was how in Israel's 2014 military assault on Gaza, numerous Palestinians were interrogated and even arrested over social media posts. Lentin also highly emphasizes that race is a very important concept in understanding Israel's system of control. She argues that surveillance in Israel's context does not merely observe, it in fact classified and dehumanizes Palestinians that are marked as threats. She then

[16] Zureik, E. (2016). Strategies of Surveillance: The Israeli Gaze. Jerusalem Quarterly, (66).
[17] Lentin, R. (2017). Race and surveillance in the settler colony: the case of Israeli rule over Palestine. Palgrave Communications, 3(1), 1-10.

explains how the scope of surveillance then extends beyond Palestinians to include international supporters of Palestinian rights, whether they are jews, human rights defenders, or others, explaining how it has become a tool of repression and censorship. Therefore, through this article Lentin demonstrates how Israeli surveillance operates to sustain a racialized settler colonial order that extends far beyond traditional warfare.[18]

Moreover, Nadim Nashif in "Surveillance of Palestinians and the Fight for Digital Rights", published in 2017, analyzes Israeli cyber surveillance techniques against Palestinians, explaining its stages during the decades-long colonial surveillance. Nashif dates back Israeli surveillance against Palestinians to the pre-state Zionist militias like the Haganah, that used to gather intel and information on Palestinians. Nashif then explains how after Israel's full occupation in 1967, it was able to evolve its surveillance techniques, primarily using low-tech tools such as the ID cards, registration of the population, watchtowers and so on. However, more recently, Israel began to utilize high-tech tools and digital instruments to conduct its surveillance. These tools include predictive policing algorithms, biometric data systems, artificial intelligence-based profiling, phone and internet eavesdropping, and widespread social media activity monitoring. [19]

This paper focuses on documentation of certain cases where Israel used its surveillance to arrest Palestinians based on their social media posts and activity. Israel's military intelligence started employing AI algorithms trained to identify key phrases like "martyr," "Zionist state," or "Al Aqsa" to scan thousands of Palestinian Facebook profiles after a wave of youth-led protests in 2015. In addition to tracking sentiment, these systems are used to forecast potential "threats" and support arrests for "incitement," a phrase that is ambiguously used to refer to a wide range of communication, including political protest. The author highlights that these activities violate fundamental legal concepts of due process, freedom of speech, and presumption of innocence. The paper also addresses Israeli intelligence use of specialized units such as Unit 8200 that deliberately use hacking, the creation of false accounts, and the monitoring of private communications to enter Palestinians' online spaces. [20]

The scholar also explains how no Palestinian that uses the internet can truly be independent of Israeli surveillance since Israel controls all infrastructure and the oversight of the digital

[18] *Ibid*.
[19] Nashif, N., & Fatafta, M. (2017). Surveillance of Palestinians and the fight for digital rights. Policy Brief, Al Shabaka, 23, 1-10.
[20] *Ibid.*

environment in the area. The paper also shows that, globally, Israel has the greatest number of surveillance tech firms per person. Cyber-surveillance exports now bring in more money for Israel's surveillance sector than conventional military weapons. The paper advocates for Palestinians to have more digital rights awareness and emphasizes the significance of international coalition building with digital rights organizations, legal reform, and digital security education.[21]

Finally, Asaf Lubin in "The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law", published in 2022, investigates the application of the right to privacy and data protection during contexts of armed conflicts. Lubin begins with critiquing how IHRL, even in its commentaries, and IHL both fail to explicitly tackle the issue of digital surveillance, even though it has become a widely used tool. Lubin argues that digital surveillance can, particularly in the context of occupation, violate autonomy and dignity in ways that are comparable to physical abuse. He uses specific examples to illustrate his argument, including the example of Palestinian civilians subjected to digital surveillance by Israeli authorities. He tackles how Israel uses several technologies to collect information on Palestinian civilians, and that could lead to arrests. Lubin uses the frameworks of both IHRL and IHL to assess the legality of such methods. In IHRL, he focuses on the rights to privacy and data protection. In IHL, he focuses on necessity and proportionality. Lubin's key finding is that during times of armed conflict, the rights to privacy and data protection must be acknowledged and enforced.[22]

Many of the existing scholars that delve into the specific Israeli cyber activities against Palestinians often provide their analysis within racial and settler-colonial frameworks, without delving into it through the lens of international law. Other scholars that do provide legal analysis do not systematically frame such practices as acts of cyber espionage within the meaning of international law. This thesis fills this literature gap through providing a deeply focused legal analysis of the Israeli cyber espionage methods, not just as surveillance, but as a deliberate, targeted intelligence operation carried out against a civilian population under occupation. In addition, it adds to the literature by clearly distinguishing between the applicable legal frameworks in the West Bank (IHRL and law of occupation) and Gaza (IHL).

---

[21] *Ibid.*

[22] Lubin, A. (2022). The rights to privacy and data protection under international humanitarian law and human rights law. In the Research Handbook on Human Rights and Humanitarian Law (pp. 462-491). Edward Elgar Publishing.

In addition to the above literature, some scholars have specifically delved into specific forms of emerging technologies and their legal implications. For instance, Arina Nachinova in her thesis titled "Facing the Future: Emerging Militarisation of Facial Recognition and Public International Law Considerations," published in 2021, provides a through legal analysis of the use of face recognition technologies (FRT) by the military in drones, autonomous and semi-autonomous weapons systems (LAWs), and other military equipment. Nachinova addresses these technologies' compatibility with both International Humanitarian Law (IHL), and International Human Rights Law (IHRL). She begins with discussing the incorporation of such technologies into military use as a developing but little-studied trend, especially by nations like the United States, China, Turkey, and Iran. [23]

According to Nachinova, the use of such equipment presents difficult legal, moral, and practical issues, particularly regarding distinction, proportionality, and human oversight in combat. The thesis first assesses the application of facial recognition under IHL, beginning with Additional Protocol I's Article 36, which mandates a legal examination of new weapons. Nachinova applies fundamental IHL principles to facial recognition-enabled technology, including the ban on violence against life and people, the principle of distinguishing between civilians and combatants, and the need for proportionality in attacks. She points out significant shortcomings, such as the fact that the present definitions of IHL are too ambiguous to address the particular operational and technical hazards associated with facial recognition systems.[24]

Then the thesis turns its attention to IHRL, exploring the potential applications of the principle of non-discrimination, the right to life, and the prohibition of cruel or degrading treatment to weapons that use facial recognition. Although IHRL's applicability during armed conflict is restricted and often contested, Nachinova points out that its applicability does not cease to apply. To demonstrate how jurisprudence on lethal force, proportionality, and oversight can influence assessments of face recognition weapons, Nachinova meticulously applies case law from the European Court of Human Rights (ECtHR) and the Inter-American Court of Human Rights (IACtHR) throughout the thesis. She comes to the conclusion that states need to provide strong domestic legal regulation, operator training, and technical safeguards because the current legal frameworks, despite their shortcomings, nonetheless impose significant limitations. The use of facial recognition weaponry runs the potential of breaching both IHL

[23] Nachinova, A. (2021). Facing the future: Emerging militarisation of facial recognition and public international law considerations (LL.M. Capstone Thesis, Central European University; Supervisor: T. Soave).
[24] *Ibid*.

and IHRL in the absence of such safeguards. The thesis thus concludes that although facial recognition technology may improve targeting accuracy, its incorporation into military equipment raises significant moral and legal issues that present challenges that current international law is insufficiently prepared to handle. Therefore, a thorough legal evaluation must come before any deployment, and it must be limited by human rights and humanitarian considerations.[25]

Such literature has begun to investigate the emergence of other forms of digital surveillance technologies, such as facial recognition, and how they are being used in military operations. However, such literature that focuses on the general debates of autonomy, targeting and accountability rarely discusses the context of occupation or law enforcement carried out by military actors in civilian environments. Therefore, this thesis fills that gap through focusing on how such surveillance tools are in fact being used as a form of daily monitoring and control of an occupied civilian population.

Therefore, the discussion on cyber activities has been going on for a while and remains an important topic to be discussed. The available literature rarely focuses on the oPt, and empirical research available frequently lacks a deep legal perspective. Significantly, there is not enough investigation of how cyber intelligence and surveillance methods against civilians in the context of occupation fit within the legal frameworks of espionage, IHL, and IHRL. Thus, this thesis fills the literature gap by offering a context-specific legal classification of Israeli cyber espionage practices, drawing the distinction between Israel's operation in the West Bank and Gaza, framing its analysis in both IHRL and IHL.

1.8 Thesis Outline

This thesis is composed of an introduction, four main chapters, and a conclusion which explains the major findings and recommendations. The first chapter is the introduction. The second chapter gives a historical overview of the legality of traditional espionage under international law. It first gives a historical overview of the origins of espionage and how international law first dealt with it. After that, it distinguishes between espionage in wartime and peacetime. Then, the chapter also differentiates between intelligence activities and espionage and points out the similarities between them. It also presents the example of Israel to illustrate the intersection between intelligence gathering and espionage. After that, the chapter delves into

[25] *Ibid.*

outlining the history of Israel's espionage activities, dating back to the pre state era, and then to the formation of main intelligence bodies like Shin Bet (Shabak), Mossad and Aman. It also talks about some specialized units within the Israeli military like Unit 8200 and Mista'arvim. Therefore, it illustrates how these intelligent bodies take part in performing espionage throughout history.

Then, the third chapter shifts focus on the technological advancements and the emergence of a world that is more reliant on technology, and thus the emergence of cyber espionage. It begins by explaining how the world shifted to become more technologically advanced, how cyberspace emerged, which paved the way for the emergence of cyber espionage. It then talks about how Israel became a cyber power. After that, the chapter focuses on the specific tools and their deployment specifically in the West Bank. It also provides documented cases of their uses and analyzes the Israeli objective behind such employment. Then, it outlines the tools and their deployment in the Gaza Strip, also analyzing the objectives behind their employment.

Chapter four then delves into the legal analysis, assessing the legality of Israel's use of cyber espionage against civilians particularly in the West Bank. It begins by giving legal context, explaining what legal frameworks are applicable there. It then assesses Israeli cyber espionage methods in accordance with IHRL, particularly the right to privacy and data protection, right to freedom of expression and participation, and the right to non-discrimination. It also assesses if Israeli cyber espionage amounts to collective punishment under IHL. Importantly, after that, the chapter also examines the methods of use of information that is derived from cyber espionage, through an assessment of the use of information to arrest and detain, for coercion and informant recruitment, and their use for targeted force and lethal operations.

Chapter five assesses the legality of Israeli cyber espionage methods used on civilians in the Gaza Strip, particularly in terms of military targeting. The chapter begins by outlining the legal framework applicable to Gaza, and then it examines how Israeli cyber espionage methods have been used as military tools. After that, the chapter assesses their legality under IHL principles of distinction, proportionality and precaution.

Finally, chapter six is composed of the conclusion which details the findings of the thesis. It also provides concrete recommendations.

Chapter Two: A Historical Overview of the Legality of Espionage in International Law with Focus on Israeli Methods

This chapter provides the historical and legal foundations that are vital to comprehend the evolution of espionage under international law. It provides an overview of the definition and origins of espionage, then explaining how international law first dealt with it. It then illustrates the differences between espionage in wartime and in peacetime according to international law. After that is discusses the differences and intersections between espionage and intelligence activities and presents several examples from historical Israeli intelligence practices that showcase the interconnection between the two. In addition, this chapter also outlines the history of the Israeli espionage, starting from the pre-state period until the establishment of the state and its formal intelligence bodies.

2.1 The History of Espionage

Firstly, this section looks at both the historical and legal evolution of espionage. It begins with showing the origins of espionage and how it was normalized and used as a part of statecraft. After that, it looks at how international law began to address the act of espionage. The importance of this section lies in establishing the groundwork needed for understanding how espionage has historically operated and how international law initially addressed its regulation.

2.1.1 Origins of Espionage

Espionage is typically defined as the gathering or attempting to gather information in territory controlled by an adverse party through an act undertaken on false pretenses or deliberately in a clandestine manner. [26]In basic terms, it is "spying", which is secretly collecting information, usually for a state's strategic advantage.[27] Fundamentally, espionage is about secrecy and deception.

Espionage as a practice can be considered as old as recorded history. It has been called "the world's second oldest profession". Instances of spying are even described throughout the Bible, for example, the Hebrew Bible tells of Moses sending spies to survey the land of Canaan.[28]

[26] International Committee of the Red Cross (ICRC). (n.d.). Rule 107. Spies. Customary IHL Database. Retrieved April 21, 2025, from https://ihl-databases.icrc.org/en/customary-ihl/v1/rule107

[27] International Spy Museum. (n.d.). Espionage facts. Retrieved from: https://www.spymuseum.org/education-programs/spy-resources/espionage-facts/

[28] Hutchins, T. E. (2021). Maritime espionage and the legal consequences of the United States' potential ratification of the United Nations Convention on the Law of the Sea. National Security Law Journal, 8(1), 1–53.

The fact that governments and military leaders have constantly used spies is verified by ancient texts and historical narratives from numerous cultures. For instance, strategist Sun Tzu (c. 5th century BCE) wrote a chapter on the use of secret spies in ancient China, underlining that the only way to learn about the enemy's motives was to use them. Therefore, back in ancient times, leaders employed clandestine operatives to obtain intelligence, from the espionage networks of the Roman and Persian Empires to the Aztecs' and medieval Japan's ninja. These early spies frequently used disguise, dishonesty, bribery, or secret codes to carry out their missions, all often at substantial personal danger.[29]

Throughout history, espionage has become more regular and fundamental to state affairs. An important point in history to the evolution of the espionage practice was the European Renaissance. Modern diplomacy and espionage developed simultaneously during the European Renaissance (15th–16th centuries). States appointed resident ambassadors who, in addition to their official duties, often gathered information in secret. The “Black Chamber”, or “Cabinet noir”, serves as an example. During that time in France, the Black Chamber was a secretive French government office tasked with reading private letters. The “cabinet du secret des Postes,” which was established under Louis XV, institutionalized this practice by opening, reading, and resealing letters without the sender or recipient's knowledge. This practice was an important part of the state's espionage efforts. Its aim was to get intelligence on foreign diplomats and political rivals.[30]Another example is Sir Francis Walsingham's espionage network in Elizabethan England back in the 16th century, which used what they called "intelligencers" all around Europe to unearth conspiracies and intercept letters.[31]

The next major development in the use of espionage throughout history was industrial warfare in the early 20th century. The technological use in espionage began during World War I (1914–1918), when telegraphy and radio communications were utilized. As a result, signals

[29] Radsan, A. J. (2007). The unresolved equation of espionage and international law. Michigan Journal of International Law, 28(3), 595–624.
[30] Kent, N. (2019). The secret world: A history of intelligence. The RUSI Journal, 164(1), 86–93. https://doi.org/10.1080/03071847.2019.1605039
[31] Mielko, T. (2023). Could Pegasus Gate have been prevented? The evolution of the export control regime for cyber-surveillance tools in Israel. Cybersecurity and Law, 9, page 27.

intelligence (SIGINT)[32]became crucial. At the same time, the war promoted the use of aerial reconnaissance and the creation of specialized military intelligence groups.[33]

Later, in the Second World War (1939-1945), espionage became more advanced with the use of codebreaking. The cracking of Germany's Enigma cipher is a major example. Germany's Enigma Cipher was an electromechanical machine used by the German Nazis during the Second World War, to encode army communications. The Germans had used modern technologies to assure its efficiency, as the machine's settings were changed daily. Therefore, the Germans believed Enigma was unbreakable, and they heavily counted on it to coordinate military operations across Europe and North Africa. However, building on the previous attempts and works of Polish and French cryptanalysts, Britain's wartime code breaking center, Bletchley Park, managed to crack the Enigma. This allowed the Allies to read the German military communication in near real time.[34]

Following that, the Cold War era (late 1940s–1990s) brought with it an unmatched expansion of peacetime espionage methods and capacities. In the aftermath of the Second World War, major powers established more permanent and worldwide intelligence services with the aim of collecting information on other states. Thus, this period witnessed the creation of bodies such as the American CIA[35], the Soviet KGB[36], Britain's MI6[37], and many others. In addition, some

[32] A crucial subcategory of intelligence collection, which entails intercepting, evaluating, and using signals—mostly electronic communications—to get tactical or strategic information.
[33] Winkler, J. R. (2009). Information warfare in World War I. The Journal of Military History, 73(3), 845–867. https://doi.org/10.1353/jmh.0.0295
[34] Sebag-Montefiore, H. (2000). Enigma: The Battle for the Code. Weidenfeld & Nicolson.
[35] The Central Intelligence Agency (CIA) of the United States was established in 1947 under the National Security Act. It was created to coordinate the nation's intelligence activities and provide strategic intelligence to policymakers. See more at the Central Intelligence Agency. (n.d.). CIA history. Retrieved from: https://www.cia.gov/legacy/cia-history/
[36] The Committee for State Security (KGB) of the Soviet Union was established in 1954. It was the main security agency for the Soviet Union, in charge of intelligence, counterintelligence, and internal security. See more at Lierens, E. (2022, July 23). KGB: History, Structure and Operations. Grey Dynamics. Retrieved from: https://greydynamics.com/kgb-history-structure-and-operations/
[37] The Secret Intelligence Service (MI6) of the United Kingdom was formally established in 1909. However, it significantly expanded its operations during and after World War II.

multinational intelligence alliances were also created, such as the "Five Eyes" that included the United States, the United Kingdom, Canada, Australia, and New Zealand[38].[39]

Nearly all states had instituted systematic intelligence collection by the middle of the 20th century, and espionage emerged as a normal although hidden aspect of international affairs. Israel joined the group of countries with strong intelligence capabilities when it formed its own intelligence community in the late 1940s and early 1950s (see Section 2.4).[40] Espionage was further advanced by the technical revolution of the late 20th and early 21st centuries (satellites, computers, and the internet), which gave rise to methods of mass surveillance, cyber espionage, and electronic eavesdropping that were unimaginable to previous generations. However, the basic idea of espionage, which is getting information that others want to hide, remains unchanged, even with these shifts in scale and means.[41]

The history of espionage outlined reveals that, while the practice's methods have developed over time, its fundamental goal, which is gaining strategic advantage through knowledge of secretive information, has remained intact. The normalization of espionage throughout cultures explains why international law was reluctant to respond: espionage was historically viewed as a necessity of establishing and maintaining states rather than a violation of the law. As the thesis progresses, this setting will assist in understanding the legal difficulties that still exist today, particularly when older norms meet new technological methods. The following section explores how early international legal frameworks approached espionage, tracing the evolution of its legal treatment prior to the digital age.

[38] The "Five Eye Alliance" was initially started as a bilateral agreement between the United States of America and the United Kingdom in 1946. However, it expanded as Canada formally joined in 1948, and both Australia and New Zealand joined in 1956. See more at: Reuters. (2025, March 6). *What is the Five Eyes intelligence-sharing alliance as Trump upends geopolitics?* Retrieved from: https://www.reuters.com/world/what-is-five-eyes-intelligence-sharing-alliance-2025-03-06/

[39] Aldrich, R. J. (2001). The UK, the USA, and the Internet: The Politics of Intelligence Sharing. Review of International Studies, 27(3), 405–428. https://doi.org/10.1017/S0260210501004057

[40] Vilasi, A. C. (2018). *The intelligence services in Israel: A short history*. Open Journal of Political Science, 7(4), 454–462. https://doi.org/10.4236/ojps.2017.74036

[41] Chicago Journal of International Law. (2021). *Rethinking espionage in the modern era*. The University of Chicago. Retrieved from: https://cjil.uchicago.edu/print-archive/rethinking-espionage-modern-era

2.1.2 Espionage in Early International Legal Frameworks: A Historical Overview

The beginnings of international law and espionage are at completely different points. While espionage has existed since the dawn of time, international law, as it is expressed in norms, conventions, or treaties, is a relatively recent phenomenon.[42]For most of the time throughout history, espionage was seen as a normal tool for managing state affairs. In the context of the laws of war, the first notable legal framework appeared. Innovative initiatives such as the Lieber Code (U.S. Civil War, 1863)[43], which acknowledged espionage as a legitimate military tactic but cautioned that a spy working under false pretenses may be put to death if apprehended. These principles were further codified in the Hague Conventions of 1899 and 1907[44]. These principles were strengthened by later international instruments on the rules of war. Although not specifically defining espionage, the 1949 Geneva Conventions implicitly acknowledge it. However, there are not many treaties that directly address espionage outside of the law of armed conflict. The 1961 Vienna Convention on Diplomatic Relations, which states that diplomats must not misuse their privileges, is noteworthy because it automatically addresses espionage[45]. If a diplomat is caught spying, the host state has the authority to declare them persona non grata and deport them. [46]

Therefore, historically, the position has been that espionage is not obviously a violation of international law that results in state responsibility, but rather that it is a crime under domestic law for which spies may be detained and prosecuted by the state they spied upon. Modern discussions have been taking place in this ambiguous legal environment, particularly when new espionage techniques and the use of cyber espionage methods that are much more advanced and legally complicated to analyze, such widespread electronic eavesdropping, push the limits of international law's definitions of basic rights such as privacy and sovereignty. The following

---

[42] See supra note 36, page 596.

[43] United States War Department. General Orders No. 100: Instructions for the Government of Armies of the United States in the Field (Lieber Code), prepared by F. Lieber (1863), art. 88.

[44] For instance, the Hague Regulations of 1907 (Annex to the Convention IV respecting the Laws and Customs of War on Land) Articles 29–31 recognized espionage in wartime without explicitly criminalizing it, defining a spy as someone who, acting clandestinely, obtains information in the zone of operations with the intent of communicating it to the hostile party. While spies were denied prisoner-of-war protections if captured in the act, this treatment reflects regulation rather than outright prohibition. See: Hague Convention IV (1907), Articles 29–31.
Hague Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907. Retrieved from: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907

[45] Vienna Convention on Diplomatic Relations, arts. 9 & 41(1), Apr. 18, 1961. Retrieved from: https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf.

[46] See supra note 28.

part will examine in more detail the difference between international law's view on espionage in wartime and peacetime. This distinction has become increasingly significant today as technological advancements have blurred the boundaries between the two.

2.2 Espionage in Wartime VS. Peacetime

This section looks at how international law distinguishes between espionage during wartime and espionage in times of peace. It begins by outlining the legal status of espionage conducted during wartime. It then delves into the more uncertain legal status of espionage in peacetime. Finally, this section looks at the occupied Palestinian territory as a case study that challenges this duality, describing it as a legal grey zone in which components of both wartime and peacetime systems apply concurrently.

2.2.1 Espionage in Wartime

Espionage is recognized as a paradoxical aspect of the legal framework during wartime. While obtaining information about the other side is regarded as a valid and even essential component of battle, espionage operators work outside of the typical protections afforded to combatants and do so at tremendous personal risk. The law of armed conflict, or international humanitarian law (IHL), expressly allows governments to use spies and other covert methods to gather intelligence on their enemies.[47]

As previously mentioned, initiatives such as the Lieber Code of 1863[48], which acknowledged espionage as a legitimate military tactic but cautioned that a spy working under false pretenses may be put to death if apprehended. The Hague Conventions of 1899 and 1907 further defined these ideas. In 1907, the Hague Regulations clarified the position of caught spies and explicitly recognized espionage as a legitimate ploy of war. "Ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible," according to Article 24 of the Hague Convention (IV) of 1907[49]. Additionally, in Article 29 of the same convention, a spy is clearly defined as someone who tries to gather intelligence in the area of operations with the goal of sharing it with the enemy by acting

[47] Beim, J. (2018). Enforcing a prohibition on international espionage. Chicago Journal of International Law, 18(2). Retrieved from https://cjil.uchicago.edu/print-archive/enforcing-prohibition-international-espionage
[48] See supra note 43.
[49] Hague Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907. Retrieved from: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907

covertly or under false pretenses. The Article also entails that if apprehended, such an individual is not entitled to the same safeguards as legitimate combatants[50]. Moreover, Article 30 articulates that a captured spy must be prosecuted before receiving any punishment[51]. Therefore, the Hague regulations attempted to create a balance which allowed states to punish enemy spies if they were discovered, while still allowing the use of espionage in war.[52]

These ideas were strengthened by later international instruments on the rules of war. For instance, in Article 5 of the Fourth Geneva Convention of 1949, it is articulated that an occupying force may suspend certain rights of civilians who are unquestionably suspected of espionage[53]. Further details regarding the status of spies are provided in Additional Protocol I to the Geneva Conventions (1977). It further emphasizes that combatants acting as spies lose their combatant immunity while spying, and therefore if captured they are not entitled to a prisoner of war status[54]. However, it also explains that if the information was gathered by a member of the armed forces and is wearing the official uniform, then that is not considered espionage, and if captured the combatant is entitled to a prisoner of war status[55].

Therefore, the law of armed conflict makes a clear distinction, espionage necessitates acting clandestinely or under false pretenses. During the duration of the espionage operation, a combatant who is apprehended while spying, for example as a soldier in enemy soil dressed in civilian clothes, is not eligible for prisoner of war status. Such a person may be prosecuted under the domestic laws of the captor. Following a fair trial, this might entail incarceration or even execution. The reasoning is that the spies lose combatant immunity since they disregarded the laws of war, particularly Article 4(A)(2) of the Third Geneva Convention which stipulates that a lawful combatant must be commanded by a person responsible for his subordinates, have a fixed distinctive sign recognizable at a distance, and carry arms openly[56]. On the other hand,

---

[50] *Ibid*. Article 29.
[51] See supra note 49. Article 30.
[52] Watkin, K. (2025, February 24). I spy: Espionage, Perfidy, and fighting in the Shadows. Lieber Institute West Point. Retrieved from: https://lieber.westpoint.edu/i-spy-espionage-perfidy-fighting-shadows/#:~:text=Such%20espionage%20is%20ordinarily%20carried,gain%20over%20by%20bribery%20or
[53] Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War, art. 5, Aug. 12, 1949, https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.33_GC-IV-EN.pdf.
[54] International Committee of the Red Cross (ICRC). (1977). *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977*. Retrieved from: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977
[55] *Ibid*.
[56] United Nations. (1949). Geneva Convention (III) relative to the Treatment of Prisoners of War, art. 4(A)(2). https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.32_GC-III-EN.pdf

a combatant who gathers intelligence while meeting the legal requirements to be a lawful combatant, is not regarded as a spy and, if apprehended, must be treated as a prisoner of war.[57]

Notably, there has been some sort of unwritten protocol between states in regard to espionage during times of conflict. States use spies even when knowing that if they were caught by the enemy, the spies will be punished. There are numerous historical examples of this. For instance, during the second World War, spies who were caught were frequently put to death or employed as double agents, yet the sending state did not view their mere presence as a violation of the laws of war. The sending state, if the spy was one of its soldiers, could even deny the individual's affiliation to protect itself from political fallout. This dynamic emphasizes how espionage is a high-risk activity that is conducted under the guise of legality during times of war: legal for the employing state, but deadly for the individual agent if caught.[58] After illustrating how international law dealt with espionage in wartime, the next section explores how it dealt with it in peacetime.

2.2.2 Espionage in Peacetime

In peacetime, espionage is far more legally ambiguous. It is generally accepted that during periods of nominal peace, meaning when there is no declared armed conflict between the two states, if spying activities are conducted, that domestic laws are employed, such as the laws pertaining to official secrets and espionage. However, the question of whether it also violates international law remains opaque. The conventional response has been that, aside from being viewed as antagonistic, and unfriendly conduct, it usually does not violate international law.[59] Therefore, there has long been a gap in international law in relation to peacetime espionage. In peacetime, no multilateral treaty forbids spying in any way, and no restriction has been established by customary international law.

This is demonstrated by the frequent occurrence of spying during peacetime. For instance, the 1960 Gary Powers incident, in which the Soviet Union shot down an American U-2 spy plane, caused diplomatic distress and humiliation, but the United States was not charged with

[57] See supra note 47.
[58] See supra note 52.
[59] See supra note 28.

violating international law as espionage. The situation was rather treated as a political issue[60]. Similarly, expulsion of the operatives and criminal prosecution of any agents identified are the typical responses to espionage rings being discovered[61], rather than an appeal to an international court[62]. Therefore, Peacetime espionage is sometimes described by legal experts as functioning in a legal void that is regulated by reciprocity and implicit standards rather than formal law.

Therefore, peacetime espionage provides room for discussion. According to a group of academics, espionage may be illegal under international law in specific situations, especially if it violates the principle of non-intervention or territorial sovereignty, such as deploying spies to operate on the territory of another state. They contend that although espionage is not prohibited by any treaty, clandestine operations may violate customary principles such as respect for sovereignty. For example, cyber incursions into another state's government networks or the placement of listening devices in their embassy could be justified as breaches of political independence or territorial integrity. The more widely held belief is that espionage does not qualify as unlawful involvement as long as it is limited to information collection and does not involve the use of force or coercion. It is also believed that as long as it is kept out of the public eye, governments implicitly accept that others will spy on them since they are also spying. This means that, practically speaking, the peacetime norm is one of mutual tolerance and concealment.[63]

The situation is shifting significantly in the face of new technologies, such as cyber espionage and mass surveillance, which blur borders between espionage, privacy rights, and sovereignty. The question of whether widespread cyber espionage and collecting information on other states or people, for example, might violate principles of IHRL and IHL is becoming more and more debated.

The distinction between espionage during times of war and peace reveals a range of legality, from acknowledged in wartime to vaguely allowed in peacetime. However, the Israeli-

[60] See more at: Leone, D. (2019, July 8). *True story: What happened when the Soviet Union shot down Francis Gary Powers' U-2*. The National Interest. Retrieved from: https://nationalinterest.org/blog/buzz/true-story-what-happened-when-soviet-union-shot-down-francis-gary-powers-u-2-66021

[61] Such as Russian spies in the United States or vice versa during and after the Cold War.

[62] See more at: Andrew, C. (n.d.). The later Cold War. Security Service M15. https://www.mi5.gov.uk/history/the-cold-war/the-later-cold-war

[63] Navarrete, I., & Buchan, R. (2018). Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions. Cornell International Law Journal, 51(3), 595–624.

controlled occupied Palestinian territory (oPt) provides a particularly difficult middle ground in this spectrum, and it can be referred to as a legal grey area. This is because the situation is neither genuine stability and peace within a typical domestic governance framework nor a full-scale international Armed Conflict in the conventional sense. Rather, it is a prolonged, belligerent occupation that conflates the legal regimes of war and peace.

After having discussed how international law dealt with espionage in both wartime and peacetime, the next section explores the differences and intersections between intelligence activities and espionage. This is specifically important because the terms are often used interchangeably. Thus, understanding the differences and the intersections is essential for analyzing state behavior and assessing the legality of modern cyber espionage practices under international law.

2.3 Intelligence Activities vs. Espionage

This section defines both the conceptual and operational difference between intelligence activities and espionage, in addition to the intersections between the two. The section first describes each concept and emphasizes the distinctions between broad intelligence collection and covert espionage. The second section puts this concept into practice by studying examples from Israeli intelligence operations.

2.3.1 Definitions and Distinctions

Although they are not mutually exclusive, intelligence and espionage have an essential connection. The wide range of actions taken by a state to obtain, examine, and apply data related to its defense, foreign policy, economic situation, or national security are collectively referred to as intelligence activities. These kinds of actions might be either overt or covert, technical or human centered. Open-source research, diplomatic reporting, military reconnaissance, signal interception, and more are among them. Espionage, on the other hand, refers especially to the subset of intelligence operations that are covert. Espionage is often used to refer to spying, which is the covert gathering of information, particularly through insider recruitment or infiltration of a target opposition.[64]

[64] Council on Foreign Relations. (n.d.). What is intelligence?. CFR Education. Retrieved from: https://education.cfr.org/learn/reading/what-intelligence

While not all intelligence gatherings are espionage, all espionage is intelligence gatherings. An example of intelligence work is when a government reads the news media and public financial data of a neighboring country to learn about its economy, using open sources. However, it is considered espionage if that government covertly compensates a member of the neighbor's finance ministry to turn over private documents. Therefore, secrecy, deception, and breaking the target's rules are what set espionage apart.[65]

Intelligence is very broad term. Human intelligence (HUMINT,)[66]signals intelligence (SIGINT)[67], imagery intelligence (IMINT)[68], and open-source intelligence (OSINT)[69] are the categories into which contemporary intelligence organizations categorize their work. Espionage is closely linked to both HUMINT, the traditional spy running agents in the field and SIGINT for cyber incursions. The crucial point is that espionage entails some degree of physical or virtual trespass against the target's protected information.[70]

In scholarly discourse, intelligence encompasses more than merely information gathering, as it also refers to the evaluation and interpretation of information. However, espionage typically only refers to the gathering stage, therefore, the actual spying operation. Intelligence analysis is simply the study of secrets that have been taken. Espionage is one means of gathering

---

[65] See supra note 28.

[66] Human Intelligence (HUMINT) refers to the collection of information from human sources. It encompasses a range of activities, including overt and clandestine operations, aimed at gathering intelligence through interpersonal contact. This method is distinct from technical intelligence disciplines such as signals intelligence (SIGINT) or imagery intelligence (IMINT). See more at: American Public University. (n.d.). *What is HUMINT and how is it used in the intelligence field?* Retrieved from: https://www.apu.apus.edu/area-of-study/intelligence/resources/what-is-humint-and-how-is-it-used-in-the-intelligence-field/

[67] Signals Intelligence (SIGINT) refers to the collection, analysis, and exploitation of information derived from electronic signals and systems used by foreign targets. This encompasses a range of sources, including communications systems, radars, and weapons systems. SIGINT provides critical insights into the capabilities, actions, and intentions of foreign adversaries, playing a vital role in national security. See more at: National Security Agency. (n.d.). *Signals Intelligence (SIGINT) Overview*. Retrieved from: https://www.nsa.gov/Signals-Intelligence/Overview/

[68] Imagery Intelligence (IMINT) is the discipline of collecting and analyzing visual representations—such as photographs and satellite images—to gather information about objects, activities, or areas of interest. IMINT sources include visual photography, infrared sensors, lasers, electro-optics, and radar systems. These sensors can be deployed from various platforms, including land, sea, air, and space. See more at: U.S. Department of Defense. (1991). *Joint Publication 3-54: Joint Doctrine for Operations Security*. https://irp.fas.org/doddir/dod/jp3-54/

[69] Open-Source Intelligence (OSINT) refers to intelligence derived exclusively from publicly or commercially available information that addresses specific intelligence priorities, requirements, or gaps. This encompasses data collected from a variety of sources, including news media, academic publications, government reports, and social media platforms. OSINT plays a crucial role in informing national security decisions and protecting national interests. See more at: Office of the Director of National Intelligence. (2024, March 8). *The IC OSINT Strategy 2024–2026*. https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf

[70] Cyber Risk GmbH. (n.d.). *From espionage to cyber espionage*. Retrieved from: https://www.cyber-espionage.ch/

information, but intelligence is a process (collection, analysis, and distribution) and an output (the intelligence report).[71]

The ultimate objective of both espionage and intelligence is the same, which is to obtain information for strategic advantage. To put pieces into the puzzle, an intelligence organization may assign one officer to gather information from public sources and another to recruit a spy. For example, Israel's Mossad (intelligence agency) is in charge of conducting espionage, which involves sending secret agents overseas, but it is also in charge of doing more comprehensive intelligence analysis and coordinating with allied services and open sources.[72]

The extent and intrusion of an activity is another factor that can clarify the divergence between espionage and other intelligence operations. While espionage usually focuses on an adversary's secrets like the leader's intents, secret plans, and confidential discussions, non-espionage intelligence gathering typically deals with aggregate or impersonal information, like the economy trends, and military movements detected via satellite.[73]

Reliability and verifiability are other operational differences. Espionage information, or a secret agent's report, can be very helpful, but it can also be deceptive because the spy may double-count or misinterpret the information. The reliability of espionage sources must be taken into consideration in intelligence analysis. Cross-checking technical or open-source information can occasionally be simpler. The result of this is that the intelligence services deal with unprocessed espionage reports in a different manner that usually need regular confirmation.[74]

Therefore, intelligence activities have become widely acknowledged as a common, even inherent, feature of the modern state. The issue that emerged from normalizing intelligence activities is that there is a blurry line between regular intelligence activities and covert espionage methods. There has also been no international consensus to clear things up. On the one hand, states openly disclose their own intelligence services and consider their operations lawful and even vital for national security. On the other hand, states strongly condemn foreign

[71] Council on Foreign Relations. (n.d.). *What is intelligence?*. CFR Education. Retrieved from: https://education.cfr.org/learn/reading/what-intelligence
[72] See more at: Jewish Virtual Library. (n.d.). *The Mossad*. Retrieved from: https://www.jewishvirtuallibrary.org/the-mossad
[73]Galpin, T. S. (2016). *The difference between intelligence and espionage*. StrategicScience.Org. Retrieved from: https://strategicscience.org/the-difference-between-intelligence-and-espionage/
[74] Friedman, J. A., & Zeckhauser, R. J. (2018). Assessing uncertainty in intelligence. Intelligence and National Security, 33(2), 232–246. https://doi.org/10.1080/02684527.2017.1360078

intelligence and prohibit any domestic support for it. According to one critic, the thinking appears to be: "We and our friends gather information; you and your type violate sovereignty." Thus, while individual countries have regulated their intelligence activities through domestic legislation, very few, if any, have signed international treaties or conventions that govern intelligence activities.[75]

Domestic legal systems codify the imbalance between how states perceive their own intelligence collecting and how they treat other countries'. A significant example is the United States' Espionage Act of 1917[76], which criminalizes the unauthorized acquisition, or dissemination of national defense secrets. The Act thus does establish a legal basis for punishing foreign espionage on US soil; however it fails to criminalize US operatives abroad. Therefore, this can be seen as a broader pattern in which nations establish legal systems to delegitimize foreign intelligence efforts while protecting their own practices from scrutiny.[77]

The normalization of intelligence activities has also created another legal issue, because many states use intelligence activities including espionage methods to gain sensitive information on individuals within their states or on foreign countries all under the guise of “national security”. This is exemplified by how the United States expanded domestic intelligence operations after 9/11, targeting individuals under broad claims of national security.[78]

Due to these differentiations outlined, discussions of espionage in international law, as in this thesis, focus precisely on those covert actions rather than all intelligence in their broadest definition. In addition, it indicates that the intelligence community of a state usually does combine both espionage and non-espionage methods.

Thus, after outlining more theoretically the differences and intersections between both intelligence activities and the act of espionage, the next section provides a real life example to help conceptualize the differences between the two.

---

[75] Pun, D. (2017). Rethinking espionage in the modern era. Chicago Journal of International Law, 18(1), 353–382. Retrieved from https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1727&context=cjil

[76] See more at: United States Congress. (1917). *Espionage Act of 1917*. Retrieved from https://d1lexza0zk46za.cloudfront.net/history/am-docs/espionage-act-1917.pdf

[77] Lebovic, S. (2023, November 26). *The song and dance of American secrecy*. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2023/11/26/espionage-act-america-secrecy-state-leaks-law-democracy/

[78] Lyon, D. (2001). *Surveillance after September 11*. *Sociological Research Online*, 6(3). https://doi.org/10.5153/sro.643

2.3.2 Illustration from Israeli Intelligence

To more clearly demonstrate the similarities and difference between espionage and intelligence activities, Israel's operations can act as a live example. Pure espionage is combined with more general intelligence and even military action in many of Israel's most famous operations.

The well-known 1956 Khrushchev Secret Speech leak serves as an example of how both espionage and intelligence intercept each other. Soviet leader Nikita Khrushchev presented a very classified speech in Moscow in February 1956, that contained very important information to the west. Within weeks, the Israeli intelligence body Mossad, was able to collect the complete text of this secret speech. After being taken to Tel Aviv, Israel shared the speech with the United States, shocking the Western governments and CIA, who had not previously had access to it. The use of human resources in dangerous areas and quick intelligence work to seize an opportunity made this operation a quintessential example of Cold War era espionage. Notably, although this was espionage, as it involved taking a classified document, it also served as an example of intelligence cooperation and diplomacy, as Israel utilized the information to strengthen its strategic alliance with the United States. Thus, this operation walked a tightrope between international intelligence cooperation and sheer espionage.[79]

Similarly, the Eli Cohen example in Syria also shows the interplay between espionage and intelligence activities. Eli Cohen's penetration of the top levels of the Syrian government is arguably Israel's most well-known spying operation. In the early 1960s, Cohen, an Israeli, won a great deal of trust in Syrian ruling circles by pretending to be a wealthy Arab expatriate under the name Kamal Amin Thaabet. He secretly shared with the Israeli intelligence, Syrian military secrets through developing contacts with Syrian political and military leaders over several years, including reportedly being considered for a deputy minister position. Israeli intelligence gained very important information from Cohen, such as details on Syrian defense plans, information on the Golan Heights, and other important issues. However, Cohen paid a big price for his espionage activities, as he was later caught by Syrian counterintelligence, taken into custody, and publicly executed for espionage in 1965. This case can be considered as one of the best examples of deep-cover HUMINT. Successfully doing this operation required deceiving people for a very long period, it also needed abilities to blend into the cultural and

[79] Patel, M. (2023, November 4). *From hashomer to nili, the history of Israeli intelligence, its successes and failures*. The Indian Express. Retrieved form: https://indianexpress.com/article/research/from-hashomer-to-nili-the-history-of-israeli-intelligence-its-successes-and-failures-9011800/

linguistic atmosphere of Syria, and massive planning.[80] It also highlights how Cohen's intelligence intersected with more general intelligence goals. Some claim that Cohen's deep knowledge of Syrian defenses helped Israel win the 1967 War.[81] This example also highlights that this type of espionage comes with great personal risk because Cohen paid with his life and his remains have never been returned to his family, even after decades of Israeli attempts to retrieve them.

Therefore, the operational differences and functional overlap between espionage and more general intelligence operations are compellingly demonstrated by the case of Israeli intelligence. The Israeli intelligence's methods use both overt and covert methods to gain important information, as was evidenced by its organizations like Mossad. It is also highly important to highlight that Mossad is not Israel's only intelligence organization. It works closely and tightly with other organizations that each have functions within the country's larger intelligence system.

To expand on this, the next section delves deeper into the historical espionage methods used by Israel from the pre-state era until its state establishment and the formation of its intelligence bodies. This is essential because Israel's early methods have laid the foundation of their current modern cyber espionage methods.

2.4 Israeli Traditional Espionage: Historical Context and Espionage Bodies

This section traces the historical development of Israel's espionage system both before and after the establishment of the state, and then the institutionalization of intelligence practices. The section begins by examining early espionage activities during the pre-state period, then turns to the evolution and distinct functions of Israel's main intelligence bodies, which are Shin Bet (Shabak), Mossad, and Aman, specifying their espionage practices. In addition, it talks about some specialized units within the Israeli military like Unit 8200 and Mista'arvim.

[80] Garza, A. de la. (2019, September 5). The true story behind the spy on Netflix. Time. Retrieved from: https://time.com/5669302/the-spy-netflix-true-story/

[81] Siegal, T. (2022, December 12). *Mossad head reveals how Syria found Eli Cohen, discloses spy's final message* . Times of Israel. Retrieved from: https://www.timesofisrael.com/mossad-head-reveals-how-syria-found-eli-cohen-discloses-spys-final-message/

2.4.1 Early Pre-State Israeli Espionage Activities

Even before Israel's existence in 1948, Israel's intelligence underpinnings were established. The Jewish community in Palestine established covert networks for information gathering on the indigenous Palestinians in the latter years of the Ottoman and British Mandate regimes. Hashomer, also known as "The Watchman," was one of the first of these groups, having been established in 1909.[82] Members of Hashomer assimilated into the local population and gathered data regarding. Hashomer developed the idea of covert tactics, such as assuming regional language, customs, and disguises. Later, some Hashomer members were involved in an espionage network during World War I called NILI, which was a pro-British spy network in Palestine that operated from 1915 to 1917 and gave the British information about Ottoman military deployments.[83]

In addition, during the British Mandate, more intelligence systems were developed, building on the earlier frameworks. The Jewish Agency's Political Department at that time established a covert Arab Section that tracked local and regional political trends and built networks of informants among Arab populations. Shai (Sherut Yediot or "Information Service"), the underground militia Haganah's intelligence unit, was established concurrently and it was in charge of security and military intelligence. Notably, individuals like Ezra Danin were instrumental in setting up networks for gathering intelligence and taking advantage of conflicts among Palestinian Arabs to strengthen the security of the Yishuv.[84]

Jewish operatives in Palestine pre 1948 also used covert methods that would later develop into the customs known as "Mista'arvim". To infiltrate Arab villages for espionage reasons, members of early groups like Hashomer, and subsequently the Haganah's Shai and specialized units like Shahar, learned Arabic and the regional dialects and customs. To obtain vital information, these agents would dress in traditional Arab clothing, adopt Arab identities, and integrate into Palestinian society. The operational idea was to have a deep cover integration into the local Arab environment for espionage and security objectives, this was already actively practiced during the British Mandate period, even though the official term "Mista'arvim" would

[82] American-Israeli Cooperative Enterprise. (n.d.). *Hashomer*. Jewish Virtual Library. Retrieved from: https://www.jewishvirtuallibrary.org/hashomer
[83] Dannies, K. (2016). Charles Boutagy and the Nili Network during World War I. *Jerusalem Quarterly*, (63). Institute for Palestine Studies. Retrieved from: https://www.palestine-studies.org/en/node/202340
[84] Black, I. (1987). The origins of Israeli intelligence. Intelligence and National Security, 2(4), 151–156. https://doi.org/10.1080/02684528708431920

not appear until later with the creation of specialized Israeli military and police units. This is still utilized until today.[85]

Later, after the establishment of the state of Israel in 1948, more organized and an advanced web of intelligence activities that use covert methods that amount to espionage were then formally created by the state.

2.4.2 Shin Bet (Shabak)

As Prime Minister at that time, David Ben-Gurion thought that it was important to restructure Israel's intelligence infrastructure as soon as the State of Israel was established in 1948. Employees of the pre-state Shai were reassigned to newly formed institutions once it was disbanded. Here, Isser Harel was assigned to create an internal security organization that would eventually be called the Shin Bet (or Shabak). Its main publicly shared goal was to maintain Israel's internal security, with a particular emphasis on counterterrorism, counterespionage, and the defense of governmental institutions.[86]

The Israeli Shin Bet is considered one of the top operational, technological, and intelligence agencies in Israel's national security framework. According to its publicly available website, Shin Bet's official main duties are counterterrorism, counterespionage, cyber defense, and safeguarding sensitive sites, high-ranking officials, and key infrastructure. In addition, currently, over 25% of its employees are working in technical positions.[87]

However, despite the public claims made by Shin Bet, its activities do employ covert methods in their intelligence gathering phase, which amounts to espionage. It has been noted that at the beginning of Shin Bet's establishment, their main goal was to keep an eye on the Arab Palestinians who were still living inside Israel's boundaries after the 1948 war. During the Cold War era, Shin Bet's focus shifted on monitoring internal dissident groups while concentrating on threats from Soviet bloc intelligence services. Significantly, after the 1967 war, where Israel gained military control over the West Bank, including East Jerusalem, and the Gaza Strip, Shin Bet extended its operations to include the newly seized areas. The organization worked in the occupied Palestinian territory through using covert methods, mainly establishing a wide

[85] Mendel, Y., & Karkabi, N. (2023). The Re-Enchantment of the Orient: Mista 'arvim and Their Special Status in Jewish-Israeli Society. The Middle East Journal, 77(2), 161-180.
[86] See supra note 72.
[87] Israel Security Agency. (n.d.). About the ISA. Retrieved from: https://www.shabak.gov.il/en/about/

network of informants and accomplices within the Palestinian society. Shin Bet's tactics included torture, blackmail, and due process abuses in the treatment of Palestinian detainees. Israel's internal security policies are still influenced by its operational strategy, which is defined by covert monitoring, and intelligence penetration of civilian populations.[88]

One of the field strategies associated with Shin Bet intelligence operations is the use of "Mista'arvim" units, who are undercover operators that integrate themselves into Palestinian communities to gather intelligence, identify targets, and enable arrests. While these units are administratively assigned to special forces branches of the military or police, their activities are tightly coordinated and supervised by Shin Bet, making them an essential component of Israel's clandestine intelligence architecture in the occupied Palestinian territories.Mista'arvim personnel are one of the most obvious examples of Israel's covert intelligence operations against Palestinian people. Whether working under the Border Police's Yamas[89] unit or the IDF's Duvdevan[90] squad, these operatives blend into Palestinian neighborhoods to conduct surveillance, gather human intelligence, and carry out arrests or killings.[91]

An example to the Mista'arvim operations is the infiltration of Al-Ahli Hospital in Hebron back in 2015. Members of the Yamas squad invaded Al-Ahli Hospital in Hebron while disguised as a Palestinian family. They entered the hospital undercover as civilians, including a woman in labor, and arrested a wounded Palestinian. During the operation, another person was shot and died for allegedly interfering. This operation demonstrated the Mista'arvim's ability to blend into civilian areas and conduct targeted arrests.[92] This is one of many of Israel's regular use of the Mista'arvim.

---

[88] Bregman, A. (2023, October 26). A little history of Shin Bet. Engelsberg Ideas. Retrieved from: https://engelsbergideas.com/notebook/a-little-history-of-shin-bet/

[89] Yamas is an elite undercover unit belonging to the Israel Border Police (MAGAV).They are highly trained in Arabic language, cultural behaviors, and street-level intelligence work. Their primary missions involve arresting individuals, and supporting broader police operations inside the oPt. See more at: New Arab. (2015). *Mista'arvim: Israel's Notorious Undercover Agents*. Retrieved from https://www.newarab.com/analysis/mistaarvim-israels-notorious-undercover-agents

[90] Duvdevan is a highly classified special forces unit of the Israel Defense Forces (IDF). It was established specifically to conduct deep undercover missions within Palestinian civilian areas, focusing on targeted killings, abductions, and surgical strikes against high-value individuals. Unlike Yamas, which focuses on arrests and counter-riot operations, Duvdevan is trained for direct action missions that sometimes involve the use of deadly force as the primary objective.See more at: New Arab. (2015). *Mista'arvim: Israel's Notorious Undercover Agents*. Retrieved from https://www.newarab.com/analysis/mistaarvim-israels-notorious-undercover-agents

[91] New Arab. (2015). *Mista'arvim: Israel's Notorious Undercover Agents*. Retrieved from https://www.newarab.com/analysis/mistaarvim-israels-notorious-undercover-agents

[92] Al Jazeera. (2015, November 13). Israeli army unit Storms Hospital and kills Palestinian. Al Jazeera. Retrieved from: https://www.aljazeera.com/news/2015/11/13/israeli-army-unit-storms-hospital-and-kills-palestinian/

In later years, Shin Bet, like other Israeli intelligence agencies, began to use and advance technology to improve its ability to acquire intelligence and, in some circumstances, conduct espionage against Palestinian civilians. This will be further elaborated in the next chapter.

2.4.3 Aman

After the establishment of Israel in 1948, the state felt necessary to form a professional and coordinated military intelligence. As a result, the Israeli Forces separated the intelligence functions from its General Staff in 1950 and established Aman, short for Agaf HaModi'in, or Military Intelligence Directorate. Many of Aman's members were previously a part of the Haganah's Shai that existed pre-1948[93].

According to its own publicly available information, Aman's main aim is to give the military and the country's political leadership intelligence. That means providing strategic and tactical intelligence to combat units and decision-makers, potentially warning them of any hostile activities. Aman's organizational structure consists of a number of highly specialized and confidential units. Unit 8200, which is in charge of cyberwarfare, signals intelligence SIGINT, and extensive data interception, is one of the most well-known. Unit 504, which is responsible for recruiting, managing, and questioning human resources, is another crucial unit. In addition, Unit 9900 specializes in geospatial intelligence.[94]

Despite being presented to the public as a traditional military intelligence agency, Aman has also used covert methods of operations. Aman has a history of engaging in psychological warfare, clandestine operations, and deep-cover espionage against hostile nations. For example, in 1954, Aman was tied to the Lavon Affair, a botched false flag operation in Egypt that targeted facilities connected to the West in an attempt to topple the Egyptian government. This incident finally led to political scandal in Israel. Beyond official conflict situations, Thus, Aman is deeply ingrained in Israel's larger strategic intelligence and covert action architecture.[95]

[93] Rodman, D. (2013). Israel's silent defender: An inside look at sixty years of Israeli intelligence. Israel Affairs, 19(2), 383–384. https://doi.org/10.1080/13537121.2013.778097
[94] Israel Defense Forces. (n.d.). Military Intelligence Directorate. Retrieved April 28, 2025, from https://www.idf.il/en/mini-sites/directorates/military-intelligence-directorate/military-intelligence-directorate/
[95] Weiss, L. (2013). The Lavon Affair: How a false-flag operation led to war and the Israeli bomb. *Bulletin of the Atomic Scientists*, 69(4), 58–68. https://doi.org/10.1177/0096340213493259

In later years, Aman expanded its capabilities beyond traditional battlefield intelligence to include advanced technological methods such as cyber surveillance, signals interception, and satellite imagery. This dimension of Aman's evolving operations will be explored further in the next chapter.

2.4.4 Mossad

During the pre-state era, intelligence had been gathered by the Shai of the Haganah and other ad hoc organizations, but after establishment, Israel wanted to have a permanent foreign intelligence service. The Central Institute for Coordination was established by Ben-Gurion in 1949 and is now generally referred to as Mossad. [96]

Mossad's stated objective is to "collect intelligence, analyze information, and perform special covert operations beyond Israel's borders to ensure the security of the State of Israel and its citizens," according to both public statements and official Israeli accounts. Its activities include gathering HUMINT, communicating with other intelligence services, engaging in clandestine diplomacy, and engaging in strategic sabotage. The Prime Minister has direct control over Mossad, ensuring that its operations closely correspond with Israel's foreign policy and national security goals. Mossad is known to have specific sections for hiring, research, and technical innovation, even though its exact internal organization is still under wraps.[97]

Besides its formally declared mission, which does publicly refer to special tasks, Mossad has developed a reputation for bold and aggressive covert operations. In the past, it focused on psychological operations, targeted killings, sabotage, deep-cover espionage, and even abductions. Sayanim, a global network of Jewish volunteers that help Mossad operatives with logistics, intelligence collection, or safehouses without being official spies, is one of its most well-known clandestine techniques.[98]

The operational ideology of Mossad combines technological innovation, human-centric espionage, and a readiness to take on risky missions in politically delicate situations.

---

[96] See more at: Black, I., & Morris, B. (1991). *Israel's Secret Wars: A History of Israel's Intelligence Services* (pp. 89–92). New York: Grove Weidenfeld.
[97] Israel Ministry of Foreign Affairs. (n.d.). Mossad – The Institute for Intelligence and Special Tasks. Retrieved from: https://mfa.gov.il
[98] Thomas, G. (1999). *Gideon's Spies: The Secret History of the Mossad* (pp. 30–43). New York: St. Martin's Press.

Mossad has gradually incorporated cutting-edge technologies into its operational toolset, including cyber capabilities, enhanced surveillance, and distant intelligence collection techniques. These advancements enabled Mossad to execute espionage operations more effectively against a broader spectrum of targets, including non-state actors and civilian networks. The following chapter will provide a more detailed overview of Mossad's technological evolution.

Therefore, after careful revision of the historical evolution of espionage with special focus on Israel, the following chapter builds on this historical and legal foundation by tracing the evolution of cyber technologies and their use in modern espionage operations.

To summarize, this entire chapter has set an important historical and legal basis for understanding the concept of espionage and how it has been regulated under international law. The chapter started by explaining the origins of espionage and how it merged. After that, it showed the difference between how international law dealt with espionage during wartime and how it dealt with it during peacetime. It showed that in wartime, IHL addresses espionage and ultimately sees it as a recognized but unprotected strategy, as if caught, the spy loses protection. On the other hand, peacetime espionage is not clearly addressed and is typically seen as a political issue rather than a legal one. The chapter then shifted to the specific situation of the oPt, where the Israeli occupation does not fit easily into either the legal categories of war or peace. That is because it is considered a prolonged belligerent occupation, which is why the oPt exists in a legal gray area where both IHL and IHRL apply concurrently.

After that, the chapter explained the conceptual difference between general intelligence efforts and espionage, explaining how intelligence gathering may use a different information-gathering tool, espionage on the other hand is distinguished by its coercive and secretive nature. Lastly, the chapter has explained the historical evolution of Israeli intelligence bodies that perform espionage, specifically the Mossad, Shin Bet, Aman, and special units within the Israeli military such as Unit 8200 and Mista'arvim. It shed light on how these intelligence bodies have historically used covert methods, usually in the context of occupation. Therefore, this chapter showed that Israel has used espionage historically against both external opponents through Mossad, and the civilian population it occupies.

Thus, this understanding of both the history and the legal foundation establishes the needed framework for the following chapter, which delves deeper into how espionage has developed

in the digital age with the emergence of cyberspace, and how Israel became a cyber power and how it uses these new technologies to conduct covert intelligence operations and cyber espionage against Palestinians.

Chapter Three: From Traditional to Cyber Espionage: Israel's Evolving Methods in the oPt

This chapter provides an analysis of the technological advancements of espionage methods and the emergence of cyberspace which has led to cyber espionage. It then delves deeper into how Israel became a cyber power on an international stage. It then illustrates the specific tools and deployment of cyber espionage methods against Palestinian civilians in both the West Bank and the Gaza Strip. It also analyzes Israel's objectives behind deploying such methods in both regions. This chapter acts as an important bridge to comprehend the legal analysis in the next two chapters.

3.1 The Rise of Cyber Espionage and Israel's Emergence as a Cyber Power

This section examines how technological advancements have shaped the recent cyber espionage methods used. From simpler ways previously used to gather intelligence and the basic covert methods of sending physical spies, to penetrating the cyberspace for such uses, it is witnessed that technological advancements have reshaped how intelligence is gathered and interpreted. Now, cyber espionage is a key component of intelligence gathering, that allows the targeting of hostile states, it also allows mass surveillance of civilian populations. Within this global shift, Israel has become known for having a significant cyber power, frequently with enormous influence in the domains of cybersecurity and cyber espionage. Over the last two decades, Israel has consciously changed its strategic focus toward high-tech intelligence capabilities. Understanding this background is critical because it lays the groundwork for how these tools and methods have been used on civilians in the oPt, to then be able to legally assess them.

3.1.1 Evolution of Cyber Espionage Technology

By the end of the 20th century, and the birth of a new technological era, the espionage sphere has witnessed a complete transformation. As more sensitive information moved to networked computers, a new area of strategic engagement, known as cyberspace, arose. Cyberspace is a dynamic, interconnected domain comprising digital networks, information systems, and the human users who interact with them. It encompasses the virtual environment where data is

created, stored, transmitted, and manipulated, underpinned by physical infrastructures and governed by both technological protocols and human activities[99].

In this cyberspace, cyber espionage has evolved as a key method of intelligence collection. It entails the covert exploitation of digital technologies and networks to get sensitive information, often for political, commercial, or military purposes, without the targeted entity's knowledge or approval.[100]

Traditional forms of intelligence and espionage did not completely disappear, however, cyber capabilities evolved into a potent complement, and in certain circumstances, a substitute. Back in the 1980s and 1990s, many intelligence agencies around the world began creating techniques for infiltrating digital systems, predicting that in the 21st century there will be a surge in hacking sponsored by states. Towards the beginning of the 2000s most documents and communications that were on paper shifted to email, digital files, and cellular networks, making them a target for those with the means to exploit them. As a result, technological advancements ranging from the telegraph to satellites to computer networks have expanded the scope of espionage over time. As espionage was formerly known to be a dangerous mission, it can now be completed remotely due to these technological advancements.[101] Therefore, the emergence

---

[99] This definition is a synthesis of multiple scholarly and institutional sources. For comparative definitions, see: Ottis, R., & Lorents, P. (2011, January). Cyberspace: Definition and implications. In Proceedings of the 5th International Conference on Information Warfare and Security (pp. 267-270). Dayton: Academic Publishing Limited. Retrieved from https://www.researchgate.net/publication/287868009_Cyberspace_Definition_and_implications , Folsom, T. C. (2007). Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality). Tul. J. Tech. & Intell. Prop., 9, 75. Retrieved from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/tuljtip9&div=5&id=&page= , Sterling, B. (2018, November 14). *The Paris Call for Trust and Stability in Cyberspace*. WIRED. https://www.wired.com/beyond-the-beyond/2018/11/paris-call-trust-stability-cyberspace/ , Silva, M. A. (2020). The fundamental conceptual trinity of cyberspace. *Contexto Internacional*, *42*(1), 9–37. https://doi.org/10.1590/S0102-8529.2019420100002 , Lippert, K. J., & Cloutier, R. (2021). Cyberspace: A digital ecosystem. *Systems*, *9*(3), 48.

[100] This definition is also a synthesis of multiple scholarly and institutional sources. For comparative definitions, see: Banks, W. C. (2016). Cyber espionage and electronic surveillance: Beyond the media coverage. Emory LJ, 66, 513. Retrieved from: https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1101&context=elj , United Nations Office on Drugs and Crime. (n.d.). Cybercrime Module 14: Key Issues – Cyberespionage. Education for Justice. Retrieved April 30, 2025, from https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html , Luma-Osmani, S., CIVULI, A., ARIFI, G., & Rufati, E. (2022). Cyber espionage consequences as a growing threat. Journal of Natural Sciences and Mathematics of UT, 7(13-14), 13-20. Retrieved from: https://eprints.unite.edu.mk/1052/1/JNSM%2013-14%20e%20formatuar-13-20.pdf , Baker, K. (2025, January 16). *Cyber Espionage Explained*. CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage/ , Brown, G. (2015). Spying and fighting in cyberspace: What is which. J. Nat'l Sec. L. & Pol'y, 8, 621. Retrieved from: https://jnslp.com/wp-content/uploads/2017/10/Spying-and-Fighting-in-Cyberspace_2.pdf

[101] Banks, W. C. (2017). Cyber Espionage and International Law. *Emory Law Journal*, 66(3), 527–573. https://scholarlycommons.law.emory.edu/elj/vol66/iss3/3/

of cyber espionage was considered as a breakthrough moment, allowing state and non-state actors to undertake intelligence operations virtually via data breaches, system intrusions, and digital surveillance, all with far lower physical risks.[102]

Therefore, modern forms of espionage are highly reliant on technological surveillance methods and tools, such as encrypted communication platforms, satellite photography, and hacker technology, which enable discrete and extensive data collecting. In addition, Artificial Intelligence (AI), which are computer systems that imitate characteristics of human intelligence, like learning, reasoning, and decision-making, with the aim of completing tasks without direct human intervention[103], in addition to big data analytics tools let intelligence agencies handle and evaluate huge amounts of information in little time. Thus, these technologies spot trends in behavior, and automate certain aspects of the monitoring process. This allows for continuous monitoring of both individuals and entire populations. [104]

Moreover, a particularly important breakthrough in cyber espionage is the use of what is known as the Advanced Persistent Threats (APTs), which has become very common and even a peculiar element of state-sponsored cyber espionage efforts. APTs are organized, multi-phased attacks that are designed to gain long-term access to a target network. They are different from traditional malware attacks because they are more persistent, covert, and specifically tailored to the target's systems, behavior, and weaknesses. Examples of APTs are APT28 (Fancy Bear)[105], APT29 (Cozy Bear)[106], APT41 (Double Dragon)[107], and Volt Typhoon[108] which have all been linked to governments in Russia and China. Typically, APTs are usually linked to

[102] Editorial Team. (2024, July 14). *The Interplay of Espionage and Technology Advancements*. Total Military Insight. https://totalmilitaryinsight.com/espionage-and-technology-advancements/
[103] Khosravi M, Zare Z, Mojtabaeian SM, Izadi R. Artificial Intelligence and Decision-Making in Healthcare: A Thematic Analysis of a Systematic Review of Reviews. Health Services Research and Managerial Epidemiology. 2024;11. doi:10.1177/23333928241234863
[104] *Ibid.*
[105] See more at: The SOC Labs Team. (2024, July 7). Understanding APT28: A Full Recap of Notorious Cyber Threat. The SOC Labs. Retrieved from: https://thesoclabs.com/understanding-apt28-a-full-recap-of-cyber-threat/
[106] See more at: Picus Security. (2024). *APT29 Explained: Cozy Bear's Evolution, Techniques, and Notorious Cyber Attacks*. Retrieved from: https://www.picussecurity.com/resource/blog/apt29-cozy-bear-evolution-techniques
[107] See more at: TheSecMaster. (2025, February 18). Double Dragon (APT41). TheSecMaster. Retrieved from: https://thesecmaster.com/blog/double-dragon-apt41
[108] Forno, R. (2024, April 1). What is Volt Typhoon? A cybersecurity expert explains the Chinese hackers targeting US critical infrastructure. UMBC. Retrieved from: https://umbc.edu/stories/what-is-volt-typhoon-a-cybersecurity-expert-explains-the-chinese-hackers-targeting-us-critical-infrastructure/

national intelligence organizations and serve geopolitical purposes such as political influence, and mass monitoring and surveillance.[109]

Furthermore, it is important to highlight that cyber espionage encompasses both traditional kinds of covert intelligence gathering and state-sponsored mass surveillance activities. That means that widespread surveillance, when utilized for strategic intelligence and carried out discreetly or without public supervision, constitutes as a form of cyber espionage.[110] This is especially true when such surveillance targets entire communities rather than just military or political leaders.

Therefore, these kinds of technological advancements have completely changed the very nature of espionage. Before, espionage that relied on physical infiltration could only gather limited and very targeted kind of information. However, cyber capabilities have now allowed for the collection and analysis of major qualities of data in real time. This new kind of espionage can now easily target entire civilian populations through mass surveillance, which blurs the line of traditional espionage against enemies and complete intrusions into civilian lives. Therefore, this major evolution raises critical legal questions about the uses of cyber espionage tools against civilians, especially since unlike how international law, even if in a limited manner, addressed physical spies, there is a lack of clear guidelines under international law that govern the use of such technologies.

Thus, after illustrating how the world shifted from traditional forms of espionage to modern ways of cyber espionage, the next section showcases how Israel specifically arose as a cyber power.

3.1.2 Israel's Strategic Shift to Cyber Espionage

Like most other nations, in its early years, Israel's intelligence was centered around HUMINT and traditional SIGINT. However, in the late 20th century and in the beginning of the 21st century, Israel made a deliberate decision to prioritize cyber and electronic means of espionage. Israel worked on developing close relationships between the military and technology entrepreneurs and companies to allow the advances to be quickly implemented into intelligence

[109] See more at: CrowdStrike. (2025, January 16). *Cyber Espionage Explained*. Retrieved from: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage/
[110] Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law, 17*(2), 187–209. https://doi.org/10.1093/jcsl/krs017

operations. The thought of concentration on technological improvement is centered in Israel's historical desire to maintain a qualitative advantage over its opponents. [111]

Israel's emergence as a cyber power has been due to multiple actions and structural advantages over the last several decades. Israel's cyber espionage capabilities are a result of the strong incorporation of cyber technologies into intelligence agencies, and a network of military units. In addition, this was further aided by technologies created by the Israeli private sector businesses, and research conducted. Therefore, in this complicated network, boundaries between public and private, domestic security and foreign intelligence are frequently blurred.[112]

Firstly, all Israeli intelligence bodies, Shin Bet (Shabak), Mossad and Aman, have all deeply incorporated many technological advancements that changed the way they gather intelligence and conduct espionage. For instance, Shin Bet has been completely shifting the way it does surveillance because of its growing incorporation of digital technologies. They have made significant investments in big data analytics, AI, and sophisticated algorithms to handle enormous volumes of data collected. [113] Similarly, Israeli foreign intelligence agency, Mossad, has been using cyber technology more and more in its clandestine operations, and sometimes even fusing it with conventional espionage. An example of this is the Mossad's involvement in the 2024 pager assaults in Lebanon where numerous Hezbollah members were killed and thousands injured in this operation when thousands of pagers and walkie-talkies were fitted with micro-explosives that were probably implanted during the production process. [114]

Moreover, Israel has developed and incorporated its advanced surveillance and security technology in both its military and government bodies. For instance, the Israeli Forces have been using very advanced facial recognition technologies, that will be further explained in the following section (see section 3.2.1). [115] In addition, the Israeli government has also been using

---

[111] Cohen, M. S., & Freilich, C. D. (2024). Israel: The Making of a Global Cyber Power. Retrieved from: https://besacenter.org/wp-content/uploads/2024/10/MSPS209web.pdf

[112] *Ibid*.

[113] Davies , H., & Abraham, Y. (2025, March 6). *Revealed: Israeli military creating chatgpt-like tool using vast collection of Palestinian surveillance data*. The Guardian. Retrieved from: https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance

[114] Guardian News and Media. (2024, September 19). *Hezbollah device blasts: How did pagers and walkie-talkies explode and what do we know about the attacks?*. The Guardian. Retrieved from: https://www.theguardian.com/world/2024/sep/18/hezbollah-pagers-what-do-we-know-about-how-the-attack-happened?

[115] Dwoskin, E. (2021, November 8). Israel escalates surveillance of Palestinians with facial recognition programs in the West Bank. *The Washington Post*. Retrieved from: https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html

surveillance tools produced by the private sector, such as advanced phone-monitoring technology and spyware systems. Israeli government has also implemented what is known as smart border technologies, including motion sensors, surveillance cameras, radar systems, and remote-controlled weapons, into its border security architecture. These tools are aided by advanced data analytics and AI technologies.[116]

Furthermore, a major example of Israel's emergence as a cyber power is Israel's work on strengthening the role of specialized military units such as Unit 8200. This unit is now considered the Israeli Force's elite SIGINT, and cyber unit, and it is crucial to Israel's cyber network.[117]

Secondly, the Israeli private sector has been highly involved in advancing the technological capabilities of Israel. It is important to highlight that the Israeli cyber ecosystem is characterized by a public-private partnership. That is directly because private businesses are typically created by former members of Unit 8200 or other intelligence units, who were in technological or combat roles. These companies create monitoring and hacking technologies that are either hired by the Israeli government or licensed abroad with government approval. The most known example is NSO Group, which was founded by former Unit 8200 members and built the Pegasus spyware, which will be explained in more detail in the following section (see section 2.2.1).[118]

Thirdly, since the early 2000s, Israel has been seen as a significant international high-tech actor, also because of its big investments in education, science, and research and development. The Israeli Forces because of its need for highly qualified and innovative personnel, has become a major driver of cyber education in the country[119]. Thus, both the government and the Israeli Forces wanted to improve Israel's civil and military cyber domains and wanted a tight collaboration with industry and academia to develop Israel's cyber capabilities.[120]

Furthermore, it is important to highlight that Israel does only not use these technologies for its own intelligence purposes, but it has also emerged as a global leader in the export of cyber

[116] Rahman, A. (2024, October 16). *Explainer: The Role of AI in Israel's Genocidal Campaign Against Palestinians*. Institute for Palestine Studies. Retrieved from: https://www.palestine-studies.org/en/node/1656285
[117] Freilich, C., & Cohen, M. (2021). *Israel: The Making of a Global Cyber Power*. Oxford University Press.
[118] See supra note 111.
[119] The Israeli Forces funded educational initiatives in public schools and has been providing cyber-related training to around 10,000 soldiers each year. See more at *Ibid*.
[120] *Ibid.*

espionage tools. Israeli companies have accounted for a big portion of the worldwide surveillance tech market, with Israel's cyber exports valued in the billions. Israel is therefore considered the world's leading exporter of spyware and digital forensics tools, with at least 56 countries getting such technologies from Israeli-linked organizations.[121]

Thus, Israel has strongly established itself as a global cyber power. Importantly, most Israel's cyber espionage tools are deployed extensively against Palestinian civilians across the oPt. The nature of the deployment, both in terms of actual methods used and the objectives behind their uses, differs between the West Bank and the Gaza Strip, which reflects the different operational and legal contexts. The next section looks closely at the key Israeli cyber espionage tools used in specifically in the West Bank, it also looks documented cases of their uses, and then analyzing the different objectives behind the deployment of cyber espionage methods in the region.

3.2 The Israeli Cyber Espionage Uses in the West Bank

This section examines the specific tools of cyber espionage that Israel deploys in the West Bank, including East Jerusalem. It explains how these tools operate and then present documented cases of their deployment against civilians. The section also analyzes the objectives behind Israel's cyber espionage employment in the West Bank.

3.2.1 Tools and Deployment

Israel has been deploying numerous tools of cyber espionage against civilians in the West Bank. There have been frequent revelations by journalists, human rights organizations, and even whistleblowers that have shed light on Israeli cyber espionage tactics targeting Palestinian citizens over the years.

A major real-life example of Israel's use of cyber espionage techniques against Palestinian civilians is its use of Pegasus spyware. Pegasus is spyware that is very advanced and that aims to secretly penetrate smartphones, and it is then able to facilitate broad surveillance without the user's knowledge. This spyware is considered dangerous because it uses zero-click attacks, meaning that it allows it to infect devices without needing the user engagement, because it attacks vulnerabilities in frequently used programs like iMessage and WhatsApp. In some

[121] Global X ETFs. (2022, June 3). *Cybersecurity in Israel: Fortifying digital defenses amid elevated risks*. Retrieved from: https://globalxetfs.co/en/cybersecurity-in-israel-fortifying-digital-defenses-amid-elevated-risks/

cases, it could also use spear-phishing assaults, which involve sending false messages with malicious links that, when clicked, install malware. [122]

Once it has been implemented on a person's phone, Pegasus can access a wide range of data and even functionalities on a target's smartphone, including reading text messages and emails, monitoring calls, collecting photos, videos, contacts, tracking GPS location, and remotely activating the phone's microphone and camera for real-time surveillance. It could also collect information from the person's application on the phone such as Facebook, WhatsApp, and Gmail. In addition to all this, Pegasus is designed to function with a small footprint, which means that the influence on device performance is not notable, and it has a self-destruct feature that erases the program if it is exposed to or loses connection to its command-and-control server.[123] Detecting Pegasus is known to be difficult due to its design, however forensic investigations by organizations such as Amnesty International have established methods for detecting remnants of the spyware on infected systems. Pegasus has also been described to use similar tactics as APTs, which were explained in the previous section.[124]

Israel's use of spyware against Palestinians was properly highlighted in 2021 when it was discovered that Pegasus spyware had been installed on the phones of several Palestinian human rights activists and politicians. Technical studies verified that at least six devices belonging to Palestinian civil society workers were infected with NSO Group's Pegasus between 2020 and 2021. Among those targeted were staff from organizations working for human rights and exposing Israeli crimes, such as Al-Haq and Addameer[125].[126]

In addition to Palestinian human rights organizations, the Palestinian Authority (PA) also revealed that Pegasus spyware had been discovered on the mobile phones of three top Foreign

---

[122] Amnesty International. (2021). *Forensic methodology report: How to catch NSO Group's Pegasus*. Retrieved from: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[123] Gurijala, B. (2021, August 9). What is pegasus? how surveillance spyware invades phones. Scientific American. Retrieved from: https://www.scientificamerican.com/article/what-is-pegasus-how-surveillance-spyware-invades-phones/

[124] *Ibid*.

[125] Both of these organizations were designated as "terrorist organizations" alongside another four Palestinian NGOs. See more at: Office of the United Nations High Commissioner for Human Rights. (2021, October 26). *Israel's "terrorism" designation an unjustified attack on Palestinian civil society – Bachelet*. Retrieved from: https://www.ohchr.org/en/2021/10/israels-terrorism-designation-unjustified-attack-palestinian-civil-society-bachelet

[126] Amnesty International. (2021, November 8). *Devices of Palestinian human rights defenders hacked with NSO Group's Pegasus spyware*. Retrieved from: https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

Ministry officials. These officials were purportedly involved in the preparation of legal cases against Israel before the International Criminal Court (ICC). The PA accused Israel of employing military-grade malware to eavesdrop on its diplomats, calling the action a "blatant and immoral violation of international law."[127]

The use of Pegasus spyware against Palestinian civilians therefore shows that, while Israel also sells Pegasus to other nations, it appears to have also used the technology inwards against Palestinians. In addition to this, it is important to highlight that Palestinians under occupation, specifically in the West Bank, are frequently forced to use Israeli-provided cell phone networks, because Israeli corporations dominate mobile infrastructure, which may aid such infiltration.[128]

There has been an international outrage on Israel's use of Pegasus against Palestinians. These cases demonstrate the severe lengths that can be used by Israel as the occupying power to monitor any form of Palestinian political dissent, viewing legitimate civil society work as something to be spied on and later suppressed. In response to this, a group published a united statement criticizing the hacking of the phones of Palestinian human rights defenders as a gross abuse of surveillance technology.[129]

Another major example of Israel's documented cases of cyber espionage against Palestinian civilians is the use of facial recognition technologies. With applications such as the Blue Wolf and Red Wolf, Israel can integrate facial photos into a real-time identification system. Blue Wolf primarily uses facial recognition to create a biometric database on Palestinians, particularly in the West Bank. It works by taking a photo of any Palestinian, anywhere, and instantly matching it to a military database of personal information and prior security ratings. According to a group of Israeli soldiers who previously served in the Israeli military, and who are now opposing the Israeli occupation, Blue Wolf's database was established by relentlessly photographing thousands of Palestinians. The database works where Palestinian individuals

[127] Associated Press. (2021, November 11). *Palestinians say Israel hacked officials' phones with Pegasus.* Retrieved from: https://apnews.com/article/technology-business-israel-software-spyware-1fab8f8b88e8a7181887728e3e6bc39d

[128] WACC. (2019, May 13). *How Israel controls Palestinian ICTs*. WACC Global. Retrieved from: https://waccglobal.org/how-israel-controls-palestinian-icts/

[129] Human Rights Watch. (2021, November 8). *Spyware used to hack Palestinian rights defenders*. Retrieved from: https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders

would be color-coded via the app, with yellow or red flashing if they are reported for arrest or questioning, and green if they are cleared. [130]

Meanwhile, Red Wolf is exclusively developed for use only at military checkpoints. According to an Amnesty International investigation, Red Wolf functions also by scanning people's faces and cross-referencing them with a military database to determine whether they should be held, permitted to pass, or highlighted for further interrogation. This method automates the decision-making process at checkpoints and eliminates human judgment, depending solely on biometric data and previous profiling.[131]

On a similar note, the Israeli army deployed face-scanning surveillance (CCTV) cameras across Hebron, which were apparently connected to the "Hebron Smart City" system. These cameras can recognize people as they approach checkpoints before they even produce their ID, and troops have claimed that technology can see into houses in some cases.[132]

Furthermore, another advanced Israeli surveillance system is known as Mabat 2000. This system is designed to enable real-time monitoring and coordination using centralized command-and-control architecture. Technically, the system consists of a network of high-resolution CCTV cameras strategically placed throughout public areas, junctions, and entry points. These cameras send live footage to centralized police control centers, where operators can monitor, record, and analyze activity around the clock. The system allows law enforcement to track movements, zoom in on specific individuals or vehicles, and effectively coordinate dispatch units. Mabat 2000 also has video preservation and replay capabilities, enabling post-event inquiry and forensic analysis.[133]

The Mabat 2000 surveillance system is specifically used in East Jerusalem, as they have been installed all over Jerusalem's Old City, particularly in areas with large Palestinian populations. The network allows for 24-hour monitoring of public locations. According to Amnesty International, the Mabat 2000 system allows Israeli authorities to identify demonstrators and put Palestinians under constant surveillance, even while they go about their regular routines.[134]

---

[130] See supra note 115.
[131] Amnesty International. (2023, May 2). Automated apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT. Retrieved from: https://www.amnesty.org/en/documents/mde15/6701/2023/en/
[132] See supra note 115.
[133] See supra note 116.
[134] See supra note 131.

Another primary method used by which Israel conducts cyber espionage on Palestinians is the regular surveillance of their social media platforms. There have been recent reports that Israel's military such as Unit 8200 has created a strong AI tool that uses a massive collection of intercepted Palestinian communications.[135]

Israel's use of this mass surveillance method is not considered passive, because it is an active means of intelligence collecting, profiling, and predictive intervention, which falls clearly under the purview of cyber espionage. The Shin Bet (Shabak) and the Israeli police, have both been relying on advanced technological digital surveillance to monitor, evaluate, and even prosecute Palestinian based on their online material. It is crucial to note that this tactic has resulted in the arrest of hundreds of Palestinians on charges of what they loosely define as "incitement," sometimes based on social media posts, likes, or shares that are seen as supportive of resistance or critical of Israeli policy.[136]

Furthermore, Israel has also been using predictive police algorithms to identify individuals who are considered potential risks for Israel simply based on their digital activities. These Israeli systems typically work without public oversight, and they majorly lack transparency in how content is chosen, flagged, and interpreted. Therefore, Palestinian individuals are frequently held in detention not for specific threats they impose, or for any planning they make, but for suspected patterns of behavior that are directly derived from their online presence. The use of such algorithms has allowed the Israeli authorities to pursue preemptive arrests based on the projected possibility of future infractions, raising serious issues about due process and the right to freedom of expression.[137]For instance, between 2015 and 2016, nearly 200 Palestinians were imprisoned due to vague incitement charges stemming from their social media activities.[138]

There are numerous illustrations. In one example, a Jerusalemite named Nader Halahleh was sentenced to seven months in prison for seven Facebook posts, each of which constituted a distinct infraction. Similarly, children such as Kathem Sbeih, aged 17, have been held under

---

[135] See supra note 113.

[136] Addameer Prisoner Support and Human Rights Association. (2018). *Arrests on charges of "incitement" on social media platforms and Israeli government policy: A Facebook case study*. Retrieved from: https://addameer.org/publications/arrests-charges-%E2%80%9Cincitement%E2%80%9D-social-media-platforms-and-israeli-government-policy

[137] Human Rights Watch. (2019, December 17). *Born without civil rights: Israel's use of draconian military orders to repress Palestinians in the West Bank*. Retrieved from: https://www.hrw.org/report/2019/12/17/born-without-civil-rights/israels-use-draconian-military-orders-repress

[138] Harel, A. (2017, May 31). *How Israel jails Palestinians because they fit the 'terrorist profile'*. Haaretz. Retrieved from: https://www.haaretz.com/israel-news/2017-05-31/ty-article-magazine/.premium/israel-jails-palestinians-who-fit-terrorist-profile/0000017f-f85f-d044-adff-fbff5c8a0000

administrative detention, which is a measure that permits prolonged imprisonment without accusation or trial, based only on intelligence reports alleging provocation on social media. Another major example was Dareen Tatour, a Palestinian poet, who was detained in 2015 for posting a poem on Facebook titled "Resist, my people, resist them." The Israeli prosecution used a mistranslated Hebrew version of her poem to claim that it was an encouragement to terrorism. Tatour was subjected to 21 days of intense interrogation, house arrest under difficult conditions, and eventually prison term, even though there was no indication of violent intent.[139]

Furthermore, post October 7,2023 Israeli authorities increased even much further their surveillance of Palestinian digital activities, specifically on social media. Ever since, there has been an increase in very vague "incitement" allegations, with hundreds of Palestinians investigated and many detained or punished just for expressing their views online.[140] Emergency legislation and new regulations have given Israeli authorities greater authority to arrest those accused of undermining "national morale" or consuming "terrorist-affiliated" content.[141]

In addition, Israeli forces have increased invasive digital surveillance methods at checkpoints throughout the occupied West Bank, including physically demanding access to Palestinian mobile phones to inspect social media information. According to documentation, troops have arrested or beaten people on the spot if they locate photographs, videos, or posts that are politically pro Palestine or pro armed resistance, for example, videotape of military atrocities or statements of solidarity with Gaza. In one example, a human rights activist was imprisoned and abused when soldiers discovered a video on her phone of the Israeli military abusing a person with disability. The activist was detained without charge for 12 days and she was refused access to a lawyer throughout that time.[142] Following the November 2023 change to Israel's

---

[139] *Ibid.*

[140] Human Rights Watch. (2024, September 10). *Questions and Answers on the Israeli military's use of digital tools in Gaza*. Retrieved from: https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza

[141] AP News. (2024, November 24). *Israel detains Palestinians over social media posts amid Gaza war*. Retrieved from: https://apnews.com/article/849cc9250534b5bae98cea89e6f4d35e

[142] Levy, G. (2025, February 1). *Israeli troops are now going through Palestinians' phones. Anything 'forbidden' provokes abuse*. Haaretz. Retreieved from: https://www.haaretz.com/israel-news/twilight-zone/2025-02-01/ty-article-magazine/.highlight/idf-troops-are-now-going-through-palestinian-phones-anything-forbidden-provokes-abuse/00000194-bfdb-dbd4-a9dc-bfdf9c740000

counter-terrorism law, which criminalizes the "consumption of terrorist materials," troops have penalized Palestinians for just having photographs of Gaza on their phones.[143]

Furthermore, it is important to note that in many cases Israel uses sensitive personal information it collects through surveillance to convert Palestinians into collaborators. To elaborate, back in 2014, 43 reserve members of Unit 8200 openly refused to continue serving specifically due to ethical concerns they had, and they provided testimonies that shed light on how Israel uses the information. They stated that Unit 8200 analysts are directed to compile sensitive facts about the lives of Palestinians, including sexual orientation, infidelity, health concerns, or financial problems, therefore, anything that could be used to "extort/blackmail the person and turn them into a collaborator."[144]

To illustrate, a young Palestinian man described such an event, saying that he was talking with someone on a dating app, where the other person was asking odd questions about the political opinions of some of his university professors. The Palestinian noted that he told the person he was texting ""why are you trying to convince me that this doctor is a bad person just because he's against the occupation? It feels weird at first. Just bizarre." After the conversation, the Palestinian was contacted by someone who later revealed himself to be an Israeli intelligence officer. Using the man's phone number, the officer had apparently accessed his Facebook account and began sending messages containing the names and photographs of his family members, even though the young man had not revealed his full identity. "I started crying. I didn't know what to do," he said. Though he blocked the officer on the dating app, the harassment continued through SMS. The officer threatened to expose the man's sexual orientation unless he cooperated. [145]

The officer then demanded that the man gather information on his cousins, who were being detained by Israel for alleged involvement in Hamas. "He told me that I should go to their homes, question their parents, and report back," he recalled. "He said, 'You can't run away from us. We know where you live.'" The most chilling part, the man explained, came when

[143] Schofield, D. (2023, December 20). *Israeli soldiers are snatching Palestinians' phones and punishing them for having photos of Gaza*. Novara Media. Retrieved from: https://novaramedia.com/2023/12/20/israeli-soldiers-are-snatching-palestinians-phones-and-punishing-them-for-having-photos-of-gaza/

[144] Beaumont, P. (2014, September 12). *Israeli intelligence veterans refuse to serve in Palestinian territories*. The Guardian. Retrieved from: https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-reservists-refuse-serve-palestinian-territories

[145] Chatelle, T. (2024, August 30). *How Israel's Elite Intelligence Unit Targets Queer Palestinians in the West Bank*. Drop Site News. Retrieved from: https://www.dropsitenews.com/p/how-israels-elite-intelligence-unit

the officer threatened: “I know you’re gay. If you don’t cooperate, I’ll tell your family and your friends. You will lose everything.” [146]

This documented case is one of many. [147] Therefore, these tactics are specially used to coerce or blackmail individuals into becoming informants, exploiting the deep social stigma and potential risks associated with for example being openly queer in the Palestinian context.

In addition to this, former Unit 8200 have also revealed that they use the information they gather through covert digital surveillance “for political persecution and to create divisions within Palestinian society by recruiting collaborators and driving parts of Palestinian society against itself.” [148]

Lastly, Israel has also been using UAVs for both surveillance and for operational purposes in the West Bank. The Israeli military uses these drones to gather intel, track movement, and observe crowds. Their frequent and noisy presence has been related with psychological stress and a sense of continuous supervision among Palestinian residents.[149] In some cases, the information gathered from surveillance drones are then used for targeted or extrajudicial killings (see section 4.4.3). Furthermore, settler councils and linked organizations use drones to monitor Palestinian building specifically in Area C of the West Bank. After that the settlers inform the military of what they see, construction wise, which then contribute to demolition procedures and hinder Palestinian development.[150]

Thus, after having established the specific cyber espionage tools Israel uses against civilians in the West Bank, the next section analyzes the objectives behind using such tools. This is important because underlying the objectives reveals the broader legal implications of cyber espionage under international law, particularly in the context of prolonged occupation.

---

[146] *Ibid.*

[147] See another example at: O'Connor, N. (2013, February 19). *Gay Palestinians are being blackmailed into working as informants*. VICE. Retrieved from: https://www.vice.com/en/article/gay-palestinians-are-being-blackmailed-into-working-as-informants/

[148] See supra note 144.

[149] See supra note 131.

[150] Hasson, N. (2020, December 31). *Israel to fund drones, patrol units to monitor unauthorized Palestinian construction*. *Haaretz*. https://www.haaretz.com/israel-news/2020-12-31/ty-article/.premium/israel-to-fund-drones-patrol-units-to-monitor-unauthorized-palestinian-construction/0000017f-f351-d5bd-a17f-f77bfe760000

3.2.2 Israeli Objectives from Cyber Espionage

The Israeli government and military frequently claim that conducting cyber espionage through monitoring Palestinians is essential for Israel's security. According to Israeli officials, these mass surveillance technologies, such as facial recognition software and extensive data collecting are "part of the fight against terrorism and the efforts to improve the quality of life for the Palestinian population in Judea and Samaria," and that they are considered "routine security operations."[151] Therefore, on one hand, Israel claims that using such technologies is a part of their broader strategy to prevent assaults and ensure public safety. On the other hand, there are numerous scholars and human rights organizations that argue that this Israeli rationale acts to hide a more complicated and even institutional Israeli logic. Thus, Israel's monitoring system acts as a tool to have holistic control. It is argued that the Israeli occupation of the across the oPt is seen as a type of "cyber occupation," in which digital surveillance is used with physical dominance to regulate and oppress the Palestinian populace. Therefore, the claim is that using this type of mass surveillance in this occupation context is not about security, it is about aiming to maintain a structure of control, repression, and population management using advanced technology.[152]

Importantly, some also argue that there is an economic and industrial logic behind Israel's cyber occupation. The argument is that the oPt serves as a testing ground for Israel's rapidly expanding surveillance and cybersecurity business. Technologies that are initially used on Palestinians are later offered globally as "field-tested," generating economic profit and increasing Israel's position as a leading producer of cyber capabilities. Human rights organizations such as Al-Haq and others argue that this ultimately serves to promote ongoing surveillance and completely blurs the boundary between any military need and commercial benefit from these techniques.[153]

More particular to the context in the West Bank, Israel can be seen to use cyber espionage tools to enforce its territorial control over the land, and to crush political suppression. It is argued

---

[151] See supra note 115.

[152] Taha, S. (2020). *The cyber occupation of Palestine: Suppressing digital activism and shrinking the virtual sphere*. Global Campus of Human Rights. Retrieved from: https://repository.gchumanrights.org/bitstreams/cdc7ea07-bb61-41f0-9a13-785aadb54b97/download

[153] Al-Haq. (2019). *Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. Retrieved from: https://www.alhaq.org/cached_uploads/download/alhaq_files/images/stories/PDF/Submission_to_the_UN_Special_Rapporteur_on_the_Promotion_and_Protection_of_the_Right_to_Freedom_of_Opinion_and_Expression.pdf

that Israeli's various mass surveillance instruments used specifically to the West Bank maintain apartheid by constantly identifying, restricting mobility, and controlling spaces.[154] In some cases the information taken from cyber espionage are used as a tool to arrest individuals[155],and in some cases for target killings[156], frequently without transparent legal processes. Therefore, the information derived from the cyber espionage in the West Bank aims to assert control.

From a legal standpoint, using cyber espionage for such purposes of monitoring, intimidate, arresting, or conducting extrajudicial killings without due process presents serious problems under international law. Therefore, such practices must be analyzed to assess their compliance with fundamental rights.

Thus, after having established the cyber espionage tools deployed against civilians in the West Bank and analyzing the objectives behind such uses, the next section looks closely at the tools, deployment and objectives in the Gaza Strip, to show the operational difference between the two regions. This in turn will lay the foundation needed to understand the difference in the legal framework and legal analysis between the two regions within the oPt.

3.3 The Israeli Cyber Espionage Uses in the Gaza Strip

This section shifts focus on the specific tools and uses of cyber espionage tools in the Gaza Strip. It provides details on the different tools employed specifically in Gaza. It also analyzes the Israeli objectives behind using such cyber espionage tools in Gaza. Given that in Gaza these tools are integrated directly into the use of force and lethal operations, more specific case

[154] See more at:
Amnesty International. (2023, May 2). Automated apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT. Retrieved from: https://www.amnesty.org/en/documents/mde15/6701/2023/en/

[155] Israeli authorities are increasingly using social media surveillance to arrest Palestinians in the West Bank. See more at: Addameer Prisoner Support and Human Rights Association. (2018, October). *Arrests on charges of "incitement" on social media platforms and Israeli government policy: A Facebook case study*. Retrieved from: https://www.addameer.org/publications/arrests-charges-%E2%80%9Cincitement%E2%80%9D-social-media-platforms-and-israeli-government-policy

[156] In the northern West Bank, Israeli forces have increasingly deployed unmanned aerial vehicles (UAVs) for both surveillance and targeted executions, indicating a significant shift in combat tactics. These operations often entail real-time monitoring of persons (often identified by digital and aerial surveillance), followed by drone strikes.See more at: Al Jazeera. (2023, June 21). *Israel launches air strike in West Bank, killing three Palestinians*. Retrieved from: https://www.aljazeera.com/news/2023/6/21/israel-air-strike-hits-suspicious-vehicle-in-west-bank-attack , Al Jazeera. (2023, December 17). *Israeli military uses drones to kill Palestinians in West Bank's Tulkarem*. Retrieved from: https://www.aljazeera.com/news/2023/12/17/israeli-military-uses-drones-to-kill-palestinians-in-west-banks-tulkarem , Defense for Children International – Palestine. (2024, August 29). *Israeli drone strike kills Palestinian brothers in massive northern West Bank incursion*. Retrieved from: https://www.dci-palestine.org/israeli_drone_strike_kills_palestinian_brothers_in_massive_northern_west_bank_incursion

examples of their deployment will be examined in detail within the subsequent legal assessment.

3.3.1 Tools and Deployment

Israeli cyber espionage tactics are not confined to surveillance and monitoring in the West Bank; they have also been widely used in the Gaza Strip, but with distinct goals and means. In Gaza, these technologies are increasingly associated with military targeting and kinetic actions.[157]

Therefore, many of the tools deployed in the West Bank, such as social media surveillance, CCTV networks, facial recognition systems at checkpoints, and surveillance UAVs, are all similarly deployed in Gaza. However, the distinction is that in Gaza, specifically during active hostilities, these tools are directly and more clearly linked to military operations.

Major examples of cyber espionage tools being deployed in Gaza are AI systems, referred to as “Lavandar”, “Where’s Daddy”, and “The Gospel.” These systems came to public attention after the Israeli military operations in Gaza post October 7th, 2023[158], when investigative journalists and human rights organizations discovered their active use. However, current study on these systems is limited, as very detailed information on them is still limited. At this point, their deployment has only been documented inside the Gaza Strip, with no confirmed reports of their use in the West Bank.

Firstly, Lavandar system, reportedly created by Unit 8200, is an AI-powered database that processes massive amounts of surveillance data, including communication metadata[159], behavioral patterns, and possibly social media activity, to algorithmically identify individuals suspected of being affiliated with specific armed groups, and then places them ok “kill lists.” Israeli use of such a program has been described as an "uncharted territory for advanced warfare.” [160] Therefore, Lavender gives each resident a "suspicion score" that indicates the

[157] See more at: Human Rights Watch. (2024, September 10). *Gaza: Israeli military’s digital tools risk civilian harm*. Retrieved from: https://www.hrw.org/news/2024/09/10/gaza-israeli-militarys-digital-tools-risk-civilian-harm

[158] Post October 7,2023 refers to recommence of active hostilities between Israel, the occupying power, and armed Palestinian groups in Gaza.

[159] Refers to data that provides information about other data, such as the time, location, sender, and recipient of a digital communication. See more at: Office of the United Nations High Commissioner for Human Rights. (2014). *The right to privacy in the digital age* (A/HRC/27/37). United Nations Human Rights Council.

[160] Raviv, Y., & Fuchs, A. (2024, April 3). *Lavender: The AI machine directing Israel’s bombing spree in Gaza*. +972 Magazine. Retrieved from: https://www.972mag.com/lavender-ai-israeli-army-gaza/

probability of involvement with armed organizations. According to reports, this tool was initially deployed in Gaza in 2021 and was active during the 2023 active hostilities. Therefore, Israeli officers set a threshold score, where anyone scoring more than that is declared a military target subject to attack.[161]

According to a report by Human Right Watch, Lavender "compiles data on the behavior and connections of large numbers of individuals to assign them a suspicion score," which means that the entire population is vetted for possible targets. According to a book written by a commander in Israel's Unit 8200, who pioneered the army's use of artificial intelligence, significant features that would add onto a person's suspicion score may include belonging to a Whatsapp group with a known militant and regularly changing cell phones and addresses. .[162]

In addition to the AI system Lavender, the Israeli military have also been using a complimentary AI tool known as "Where's Daddy?" This particular tool was made to trace the movements of Palestinian individuals marked by Lavender and inform military forces when they returned home, particularly at night. This tool aimed to directly attack people while they were at home with their families, because this specifically increases the chances of killing the desired target.[163] According to reports, this tactic frequently resulted in considerable civilian losses, since airstrikes on residential buildings were launched without hesitation. An Israeli intelligence officer stated that it was "much easier to bomb a family's home" and that the system was designed to hunt for targets in these situations. Thus, in the case of Where's Daddy? the system employs real-time surveillance and digital tracking technologies to track the movements of people already identified by the Lavender AI system. It collects and analyzes SIGINT, which may include intercepted phone records, geolocation, and behavioral patterns, to detect when targets return home—often at night with their families present. [164]

In addition, documents, media reports and testimonies from former Israeli intelligence officers, have all shed the light on another algorithmic targeting tool base on cyber espionage known as

---

[161] Abraham, Y. (2024, April 3). *'Lavender': The AI machine directing Israel's bombing spree in Gaza*. +972 Magazine. Retrieved from: https://www.972mag.com/lavender-ai-israeli-army-gaza/

[162] Abreu, M., Delpuech, A., Layan, E., Batrawi, W., Rueckert, P., Jurado, S. Á., Youssef, Y., Osman, H., Abraham, Y., Carpentier, A., & Zerrouky, M. (2024, July 25). *Death from above: How Israeli drones are killing journalists in Gaza*. Arab Reporters for Investigative Journalism (ARIJ). Retrieved from: https://arij.net/investigations/gaza-project/en/israeli-drones/index.html

[163] Democracy Now! (2024, April 5). *Lavender & Where's Daddy: How Israel used AI to form kill lists & bomb Palestinians in their homes.* .Retrieved from: https://www.democracynow.org/2024/4/5/israel_ai

[164] Rommen, R. (2024, April 7). *Israel's 'Where's Daddy?' AI system helps target suspected Hamas militants when they're at home with their families, report says*. Business Insider. Retrieved from: https://www.businessinsider.com/israel-ai-system-wheres-daddy-strikes-hamas-family-homes-2024

"The Gospel." This system, which also seems to be created by Unit 8200, processes big amounts of surveillance and intelligence data to generate a list of potential strike targets. According to sources, "The Gospel" has been used to generate strikes on what were classified as "power targets," meaning civilian infrastructure are attacked.[165] Some describes this tool's as being able to "processes enormous amounts of data that tens of thousands of intelligence officers could not process."[166]

In addition to the use of AI tools, Israel's use of surveillance UAVs in Gaza is significantly more notable, and it is very deeply integrated in its military strategy. These UAVs in Gaza operate at numerous tactical and strategic levels, as they range from non-armed to armed surveillance drones. Some surveillance drones Israel uses like "Elbit Skylark," contains only surveillance abilities and it is not capable of conducting attacks itself. Such surveillance drones are equipped with high quality cameras and are used by ground troops.[167] Meanwhile, armed drones also range in their targeting capabilities. For instance, tactical quadcopters, which are commonly modified from consumer models such as DJI drones, have high-resolution cameras and AI-enhanced object identification capabilities, meaning that they allow for close-range surveillance and precision monitoring of people and small regions.[168] These drones are armed with small shells or designed for attacks like those conducted by snipers. On the other hand, larger military surveillance UAVs, such as the Hermes 900 (Kochav)[169] and the IAI Heron, serve as long durability platforms capable of maintaining a continuous aerial presence over huge areas[170].

Importantly, there is a connection between the AI tools and the surveillance drones. Data from surveillance drones, for example, real-time video imagery, is transferred to specialized Israeli

---

[165] Human Rights Watch. (2024, September 10). *Questions and answers: Israeli military's use of digital tools in Gaza*. Retrieved from: https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza

[166] Davies, H., McKernan, B., & Trew, B. (2023, December 1). *'The Gospel': How Israel uses AI to select bombing targets*. The Guardian. Retrieved from: https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets

[167] DIMSE. (n.d.). Skylark mini UAV. Defense & Intelligence Military Systems & Equipment (DIMSE). Retrieved from: https://dimse.info/skylark-mini/

[168] Al Jazeera. (2025, May 8). *Israel retrofitting DJI commercial drones to bomb and surveil Gaza*. Retrieved from: https://www.aljazeera.com/news/2025/5/8/israel-retrofitting-dji-commercial-drones-to-bomb-and-surveil-gaza

[169] Army Recognition. (2024, April 9). Israel strengthens aerial capabilities with new Hermes 900 Star drone squadron. Defense News Army 2024. Retrieved from: https://armyrecognition.com/news/army-news/2024/israel-strengthens-aerial-capabilities-with-new-hermes-900-star-drone-squadron

[170] Jerusalem Post. (2023, November 22). How Israel's Heron drone has changed the way the IDF fights wars. The Jerusalem Post. Retrieved from: https://www.jpost.com/israel-news/article-774574

intelligence, where it is processed using AI-assisted platforms like Lavandar, Where's Daddy? and the Gospel. Thus, these systems merge all the data taken like live drone imagery with intercepted communications, pattern-of-life data, and other metadata to produce automatic target lists, that can then be used for targeted killings in Gaza.[171]

Thus, all these deployments of advanced AI-powered targeting systems and military UAVs have raised major legal questions, specifically over the concepts of distinction and proportionality and precaution under IHL. In addition, since these AI tools are relatively new, or at least newly brought to light, a clear assessment of the legality of their uses against civilians becomes very essential.

Therefore, after having examined the specific cyber espionage tools used in Gaza, the next section analyzes the objectives behind their use, which is essential to understand before the detailed legal assessment in the next chapters.

3.3.2 Israeli Objectives from Cyber Espionage

Similar to the West Bank, Israel also claims that its use of cyber espionage tools in Gaza is related to security reasons. In addition, they are also used to gain more economic profit as Israel exports these tools, marketing them as "field tested." However, what distinguishes the cyber espionage methods used in Gaza is that it goes beyond traditional cyber espionage by incorporating intelligence directly into lethal decision-making, turning the surveillance into strike commands. This means that these tools represent a militarized progression of cyber espionage, in which espionage is used as a method to carry out targeted kills rather than the final goal itself.

Therefore, in Gaza, cyber espionage tools serve a distinct strategic purpose, which is precisely military dominance. Israel's cyber espionage operations in Gaza are an operational fusion of cyber espionage with kinetic military action. Many reports suggest that thousands of people were added to kill lists solely based on computer analysis, raising worries about the automation of extrajudicial targeting and the institutionalization of collective punishment. The magnitude

[171] See supra note 163.

and opacity of these AI systems indicate that Gaza serves as a testing ground for predictive targeting and military research.[172]

In addition, these Israeli cyber espionage tools deployed in Gaza also contribute to a broader military doctrine that emphasized the need to have technical superiority and quick, reactions based on algorithms. Therefore, such cyber espionage techniques show a shift in Israeli military strategy as it is further relying on data-driven technologies to make real-time decisions in high-density battle zones like Gaza. Even though some might argue that such tools improve efficiency and precision.[173] Others still warn that technology reduces complicated human assessments to binary output, raising questions about reliability and accountability.[174]

Thus, this chapter in total looked at how espionage has grown in the digital age, and how it became more sophisticated having different forms of cyber espionage. It showed how the rise of cyberspace has turned espionage from a physically risky task to a remote, automated, and frequently blanket behavior. After that, the chapter examined more specifically how Israel became a cyber power.

After that, the chapter examined the specific tools Israel used to conduct cyber espionage against civilians firstly in the West Bank, while highlighting detailed cases. It also analyzed the Israeli objective behind its cyber espionage there. Following that, it shifted the focus on the Gaza Strip, also presenting the tools used in Gaza's context, then analyzing the Israeli objectives.

Thus, this detailed description of Israeli cyber espionage techniques highlights the importance of doing a legal assessment of their compliance with international law. Even though it is true that international law has yet to define clear, binding standards that explicitly control cyber

---

[172] See more at: Raviv, Y., & Fuchs, A. (2024, April 3). *Lavender: The AI machine directing Israel's bombing spree in Gaza*. +972 Magazine. https://www.972mag.com/lavender-ai-israeli-army-gaza/, Democracy Now! (2024, April 5). *Lavender & Where's Daddy: How Israel used AI to form kill lists & bomb Palestinians in their homes*. https://www.democracynow.org/2024/4/5/israel_ai, Rommen, R. (2024, April 7). *Israel's 'Where's Daddy?' AI system helps target suspected Hamas militants when they're at home with their families, report says*. Business Insider. https://www.businessinsider.com/israel-ai-system-wheres-daddy-strikes-hamas-family-homes-2024-4 ,Rahman, A. (2024, October 16). *Explainer: The Role of AI in Israel's Genocidal Campaign Against Palestinians*. Institute for Palestine Studies. https://www.palestine-studies.org/en/node/1656285

[173] See more at: Here is the APA citation for the source you provided:
U.S. Army Field Artillery School. (2024, March 1). *Enhancing tactical-level targeting*. Line of Departure. Retrieved from: https://www.lineofdeparture.army.mil/Journals/Field-Artillery/FA-2024-Issue-1/Enhancing-Tactical-Level-Targeting/

[174] See more at: ICRC. (2024, September 4). *The risks and inefficacies of AI systems in military targeting support*. Humanitarian Law & Policy Blog. Retrieved from: https://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/

espionage and other developing digital technologies, this does not imply that such actions operate in a legal vacuum. On the contrary, existing concepts of IHL and IHRL are still very relevant and applicable.

As a result, the following chapter will investigate whether Israel's cyber espionage practices in the West Bank comply with key legal appropriate principles under international law.

Chapter Four: Legal Analysis of Israeli Cyber Espionage Practices in the West Bank

This chapter delves deep into assessing the legality of Israel's cyber espionage methods it uses against Palestinian civilians in the West Bank. This chapter starts by outlining the legal context of the West Bank and the applicability of both IHRL and IHL. Even though both bodies of law apply, this chapter focuses primarily on IHRL, which is the more applicable framework given that Israel's operations in the West Bank are based on law enforcement rather than actual hostilities. Therefore, the analysis will focus on core IHRL principles such as privacy, freedom of expression, and equality and non-discrimination. However, one critical element of IHL, which is the prohibition of collective punishment, will be also addressed, as it is still extremely relevant. In addition, this chapter will also assess the legality of what can be done using the information gathered by cyber espionage tools in the West Bank. This includes detention, coercion and recruitment of informants and even targeted killings.

4.1 Legal Context

To fully assess the legality of Israel's cyber espionage tactics in the West Bank, firstly there needs to be an understanding of the larger legal framework that governs the territory. The West Bank is more than just a disputed zone, it is a territory that has been under prolonged military occupation, governed by distinct international legal frameworks. That is why it is crucial to first define the legal status of the West Bank and the relevant international legal frameworks.

4.1.1 The West Bank as Occupied Territory

Firstly, the West Bank, including East Jerusalem, is an area that is recognized by international law as an occupied territory that has been under Israeli military authority since 1967. That is why Israel is clearly recognized as the occupying power in the area and is therefore subject to belligerent occupation law. This has been repeatedly reaffirmed by the International Court of Justice (ICJ) and other UN organs emphasizing that this legal instrument applies to the oPt.[175]

[175] See examples affirming the applicability of the law of occupation to the West Bank, including East Jerusalem, at: International Court of Justice. (2004). *Legal consequences of the construction of a wall in the Occupied Palestinian Territory, Advisory Opinion*. Para 78. Retrieved from: https://www.icj-cij.org/en/case/131/advisory-opinions , United Nations Security Council. (2016). *Security Council resolution 2334 (2016)*. Retrieved from: https://www.un.org/webcast/pdfs/SRES2334-2016.pdf , United Nations General Assembly. (2004). *Resolution 58/292: Status of the Occupied Palestinian Territory, including East Jerusalem*. Retrieved from: https://undocs.org/A/RES/58/292, United Nations General Assembly. (2024). *Resolution A/RES/ES-10/24: Illegality of Israel's presence in the Occupied Palestinian Territory, including East*

This means that Israel, as an occupying authority, has very specific obligations to the Palestinian civilian population, who are supposed to be protected persons under GCIV.[176] In addition, Israel's duties under the GCIV enhance the previous Hague Regulations, which are considered part of customary international law and are enforceable on Israel as the occupying power.[177] Furthermore, the UN Security Council and General Assembly have repeatedly referred to the West Bank as occupied territory and have also urged Israel to fully comply with occupation laws[178].

It is very important to highlight that under occupation law, the West Bank is not seen as an active battlefield in the classic sense. That is because it is an area that has been under prolonged military rule where active hostilities between Israel and organized Palestinian armed groups are few. To put things into perspective, while there have been periodic armed clashes in the West Bank since the end of the Second Intifada, the West Bank is not classified as a zone of active hostilities under international humanitarian law. Under such conditions, the law enforcement paradigm takes precedence over the conduct-of-hostilities paradigm. What this entails is that Israel's use of force in the West Bank should normally be limited by international human rights law standards. For instance, Israel's use of force must only be used when absolutely required, considering lethal force allowed only as a last resort to protect life. In addition, the principle of proportionality should be applied. The principle of proportionality in this case refers to the degree of threat posed, rather than any strategic or military purpose. As

---

Jerusalem.Retrieved from: https://undocs.org/en/A/RES/ES-10/24, United Nations General Assembly. (2024). *Resolution A/RES/ES-10/24: Illegality of Israel's presence in the Occupied Palestinian Territory, including East Jerusalem*. Retrieved from: https://undocs.org/en/A/RES/ES-10/24, Office of the High Commissioner for Human Rights. (2024, July 19). *UN experts hail ICJ declaration on the illegality of Israel's presence in the Occupied Palestinian Territory*. Retrieved from: https://www.ohchr.org/en/press-releases/2024/07/experts-hail-icj-declaration-illegality-israels-presence-occupied

[176] International Court of Justice. (2024, April 30). *Alleged breaches of certain international obligations in respect of the Occupied Palestinian Territory (Nicaragua v. Germany), Order on provisional measures*. Retrieved from: https://www.icj-cij.org/case/193

[177] European Coordination of Committees and Associations for Palestine. (2014, January 29). *Israel's obligations as an occupying power under international law, its violations and implications for EU policy*. Retrieved from: https://www.eccpalestine.org/israels-obligations-as-an-occupying-power-under-international-law-its-violations-and-implications-for-eu-policy/

[178]See, e.g.,UN Security Council Resolution 242 (1967), S/RES/242, 22 November 1967 (affirming the "inadmissibility of the acquisition of territory by war" and calling for Israeli withdrawal from territories occupied in the conflict), UN Security Council Resolution 338 (1973), S/RES/338, 22 October 1973 (calling for implementation of Resolution 242 and negotiations under UN auspices), UN Security Council Resolution 2334 (2016), S/RES/2334, 23 December 2016 (reaffirming that Israel's settlement activity in the occupied Palestinian territory, including East Jerusalem, has no legal validity and constitutes a flagrant violation under international law; also reaffirming the applicability of the Fourth Geneva Convention to the occupied Palestinian territory), UN General Assembly Resolution 73/98 (2018), A/RES/73/98, 7 December 2018 (reaffirming the applicability of the Fourth Geneva Convention to the occupied Palestinian territory, including East Jerusalem), UN General Assembly Resolution 77/24 (2022), A/RES/77/24, 30 November 2022 (reiterating the legal status of the territory as occupied and calling for Israel's compliance with international humanitarian law and human rights law),

a result, there are more restrictions rather than the more permissive laws of warfare that apply to active combat. [179]

Therefore, the law of occupation under the GCIV of 1949 does govern Israeli action in the West Bank. However, not all the Convention's obligations apply during a prolonged occupation with no active hostilities. According to Article 6 of the GCIV, the entire Convention continues to apply in its full form for the first year after the end of active hostilities, however, only certain articles continue to apply after that period in cases of continuing occupation without ongoing military operations, referring to active hostilities.[180]

The Commission of Inquiry has expressed concern stating that "Israeli authorities are increasingly applying the conduct of hostilities paradigm to the West Bank, causing West Bank operations to increasingly resemble those carried out in Gaza."[181]

Therefore, the current situation in the West Bank is one of occupation, with policing and security operations targeting people or small groups rather than open armed hostilities between troops. As a result, law enforcement under IHRL prevails in the West Bank. Occupying forces are required to police the region in good faith, maintaining public order while preserving the fundamental rights of civilians. Any undue militarization of law enforcement or treating people as combatants in the absence of an active conflict, would contravene this legal setting.

Thus, after establishing the applicability of both IHRL and IHL in the West Bank, the next section examines the specific legal framework in greater detail, identifying which elements are most relevant and how they apply in practice.

4.1.2 Applicable International Legal Frameworks

The context of the West Bank combines two complementary frameworks of international law, which are IHL, specifically the law of occupation applicable even when there are no active hostilities as outlined in Article 6 of GCIV, and IHRL. The ICJ's jurisprudence, for instance,

[179] See more at: United Nations General Assembly. (2023, September 5). *Report of the Independent International Commission of Inquiry on the Occupied Palestinian Territory, including East Jerusalem, and Israel* (A/78/198). Retrieved from: https://documents.un.org/doc/undoc/gen/n23/260/71/pdf/n2326071.pdf?
[180] International Committee of the Red Cross (ICRC). (1949). *Geneva Convention relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention)*. Retrieved from: https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949
[181] See supra note 179, par.35.

in both the 2004 Wall Advisory Opinion[182] and the 2024 Advisory Opinion on the legal consequences of Israel's occupation, has confirmed that human rights treaties, as well as certain provisions of IHL[183], continue to apply in occupied territory. Therefore, the human rights convention protections do not stop to be applicable during military occupation, instead, both IHL (some and not all provisions) and IHRL are co-applicable. Therefore, the most important thing to highlight is that occupation does not create a legal vacuum, instead the occupying power is governed by the full spectrum of international law applicable to its conduct.[184]

To break it down, under IHL, Israel's activities in the West Bank are governed by the Hague Regulations of 1907, as it is considered customary international law, and some provisions of the GCIV. For instance, Article 42 of the Hague Regulations defines occupation, and Article 43 imposes a duty to restore and maintain public order and civic life while respecting, to the greatest possible extent, the laws in force before in the territory occupied.[185] The GCIV, to which Israel is a signatory party to, specifically protects civilians in occupied territory, outlining extensive provisions on their rights and the occupying power's obligations.

Article 154 of the GCIV obviously states that it supplements the Hague Regulations of 1907, namely Section III on military occupation.[186] These two instruments together constitute the primary legal framework governing hostile occupation. The ICJ confirmed this in its 2004 Advisory Opinion that the Hague Regulations are part of customary international law and hence enforceable on Israel as an occupying power.[187] As a result, Israel is unable to evade the legal

[182] The ICJ reaffirmed that both international humanitarian and human rights law continue to apply concurrently (International Court of Justice, 2004, paras. 106–10, 113). See more at: International Court of Justice. (2004, July 9). Legal consequences of the construction of a wall in the Occupied Palestinian Territory (Advisory Opinion). Retrieved from: https://www.icj-cij.org/sites/default/files/case-related/131/131-20040709-ADV-01-00-EN.pdf

[183] The ICJ reaffirmed that both international humanitarian and human rights law continue to apply concurrently (International Court of Justice, 2024, paras. 99–100, 269). See more at: International Court of Justice. (2024, July 19). Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem (Advisory Opinion). Retrieved from:https://www.icj-cij.org/sites/default/files/case-related/186/186-20240719-adv-01-00-en.pdf

[184] See supra note 180, and International Court of Justice. (2024, July 19). Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem (Advisory Opinion). Retrieved from https://www.icj-cij.org/node/204176

[185] International Committee of the Red Cross. (1907). Hague Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. Articles 42–43. Retrieved from https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907

[186] International Committee of the Red Cross. (1958). *Commentary on the Fourth Geneva Convention*. Retrieved from: https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-154/commentary/1958

[187] International Court of Justice. (2004). *Legal consequences of the construction of a wall in the Occupied Palestinian Territory, Advisory Opinion*. ICJ Reports 2004, p. 89. Retrieved from: https://www.icj-cij.org/en/case/131

limits imposed by the law of occupation. In the occupied West Bank, where no active hostilities are taking place, only specified GCIV provisions remain in effect after the first year of occupation, as outlined in Article 6. The specific Articles of GCIV that do apply in the occupied West Bank are Articles 1–12, 27, 29–34, 47, 49, 51, 52, 53, 59, 61–77, and 143. The applicability of the provisions stated in Article 6 to the occupied West Bank was also affirmed in the ICJ's 2004 advisory opinion, paragraph 125.[188]

As a result, Israel's cyber espionage methods used on Palestinians must be investigated in accordance with these obligations—such as Article 27 (humane treatment), Article 31 (prohibition of coercion), Article 32 (prohibition of measures causing physical or moral suffering), and Article 33 (prohibition of collective penalties), as well as applicable customary IHL rules, including those reflected in the Hague Regulations.[189]Therefore, any cyber espionage that ends in inhumane treatment, intimidation, or other forbidden conduct under IHL would be a breach of Israel's obligations as an occupying power in the occupied West Bank.

Besides IHL, Israel is also a party to fundamental human rights treaties that also apply to people that are under its military rule in the occupied West Bank. For instance, among these are the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social, and Cultural Rights (ICESCR), and the Convention on the Rights of the Child (CRC). Moreover, some treaty organizations, such as the UN Human Rights Committee, has highlighted regularly that a state's human rights duties still do apply to areas under its effective authority, such as the West Bank in relation to Israel, even if they are not directly within its sovereign borders[190]. Therefore, this means that Palestinians in the West Bank are

[188] International Court of Justice, Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 2004, para. 125. Retrieved from: https://www.icj-cij.org/en/case/131/advisory-opinions

[189] See supra note 180.

[190] See, e.g., *UN Human Rights Committee, General Comment No. 31*, The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13 (2004), para. 10 (affirming that the ICCPR applies to anyone within the power or effective control of a state, even outside its territory); *UN Human Rights Committee, Concluding Observations on Israel*, CCPR/C/ISR/CO/4 (2014), para. 5 (reiterating that the ICCPR applies to the occupied Palestinian territory, including East Jerusalem); *ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, ICJ Reports 2004, paras. 106–113 (affirming concurrent applicability of IHRL and IHL in occupied territory); *ICJ, Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem*, Advisory Opinion (2024), paras. 99–100, 269.

indeed entitled to the rights provided by these treaties, which Israel must respect and enforce without discrimination[191] and to the full extent of its jurisdiction.

There are essential human rights that are relevant to cyber espionage, and they include the right to privacy (ICCPR art. 17), freedom of expression (art. 19), freedom of peaceful assembly (art. 21) and association (art. 22), the right to liberty and security of persons (art. 9), the right to life (art. 6), and the rights of minors (ICCPR art. 24; CRC provisions).[192]

It is important to shed light on the fact that for very long, Israel has continuously proclaimed that the ICCPR does not apply extraterritorially, and it says that the international treaty's precautions only apply to those who are on its sovereign territory and are subject to its jurisdiction.[193] However, this position has been explicitly rejected by the ICJ. This was affirmed in its 2004 Advisory Opinion[194], in addition to its 2024 Advisory opinion[195], emphasizing that the ICCPR applies to acts carried out by a state in the exercise of its authority, even if those acts occur outside its national territory.

Israel's refusal to acknowledge the ICCPR's extraterritorial application is also directly related to its broader argument that the West Bank is a zone of ongoing hostilities rather than an

[191] See more at: United Nations General Assembly. (1966). *International Covenant on Civil and Political Rights*. Treaty Series, vol. 999, p. 171. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights and United Nations General Assembly. (1965). *International Convention on the Elimination of All Forms of Racial Discrimination*. Treaty Series, vol. 660, p. 195. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial

[192] United Nations General Assembly. (1966). *International Covenant on Civil and Political Rights*. Treaty Series, vol. 999, p. 171. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[193] See more at: International Commission of Jurists. (2020, June). *Israel: Ensure full compliance with the International Covenant on Civil and Political Rights* [Advocacy Analysis Brief]. International Commission of Jurists. Retrieved from: https://www.icj.org/wp-content/uploads/2020/06/Israel-ICCPR-compliance-Advocacy-Analysis-Brief-2020-ENG.pdf and United Nations Human Rights Committee. (2014, November 21). *Concluding observations on the fourth periodic report of Israel* (CCPR/C/ISR/CO/4). United Nations. https://www.un.org/unispal/document/auto-insert-180034/

[194] The Court affirmed this principle in paragraph 111 of the 2004 Advisory opinion. See more at:International Court of Justice. (2004, July 9). *Legal consequences of the construction of a wall in the Occupied Palestinian Territory (Advisory Opinion)*. ICJ Reports 2004, p. 136. Retrieved from: https://www.icj-cij.org/sites/default/files/case-related/131/131-20040709-ADV-01-00-EN.pdf

[195] The Court affirmed this principle in paragraph 100 of the2024 Advisory opinion. See more at: International Court of Justice. (2024, July 19). *Legal consequences arising from the policies and practices of Israel in the Occupied Palestinian Territory, including East Jerusalem (Advisory Opinion)*. Retrieved from: https://www.un.org/unispal/wp-content/uploads/2024/07/186-20240719-adv-01-00-en.pdf

occupied area regulated by law enforcement standards. Israel's aim from this is to avoid the more protective and restrictive duties that come with IHRL.[196]

The applicability of both IHL and IHRL in the occupied West Bank is incredibly important to shed light on because it requires Israel's cyber espionage tools and techniques to be legal under both regimes. If a cyber espionage method breaches human rights, then it is not excused by the existence of an occupation or security justifications. Instead, that would represent a violation of Israel's IHRL responsibilities in addition to any IHL analysis.

Thus, after establishing the applicable specific legal frameworks that govern the West Bank, the next section addresses the legal implication of Israel's development of cyber espionage tools against the Palestinian civilians. Even though both IHRL and IHL apply to the West Bank, the next section places special focus on IHRL as it provides the primary framework governing law enforcement conduct in the West Bank and a more appropriate lens for assessing the legality of cyber espionage practices targeting a civilian population outside active hostilities.

4.2 Legal Assessment of the Israeli Uses of Cyber Espionage in the West Bank

After explaining the legal frameworks applicable in the occupied West Bank, this section addresses the legal implications of Israel's cyber espionage in the area as separate acts under IHRL, regardless of the outcomes that such espionage may produce. The question here is whether the act of cyber espionage itself violates internationally protected rights. This section looks at key IHRL principles such as the right to privacy and data protection, the right to freedom of expression and other related rights, and the right to equality and non-discrimination. Under IHL, the section looks at if Israel's cyber espionage tools against civilians in the West Bank amounts to collective punishment.

4.2.1 Privacy and Data Protection

The right to privacy is a fundamental human right that is guaranteed by Article 17 of the ICCPR, which states that "no one shall be subjected to arbitrary or unlawful interference with

[196] See more at: Diamond, E., Nohle, E., & Schmidl, A.-C. (2025, January 30). *The legal framework regulating Israel's use of force in the West Bank*. Opinio Juris. Retrieved from: https://opiniojuris.org/2025/01/30/the-legal-framework-regulating-israels-use-of-force-in-the-west-bank/

his privacy, family, home, or correspondence." In addition, it highlights that everyone has the right to legal protection against such interferences.[197]

Even though this principle was established long before the digital age, the international community considering these technological advancements has clearly reaffirmed this freedom. As an example to this, the UN General Assembly in its Resolution 68/167 (2014) specifically on the right to privacy in the digital age recognizes that the same rights people have offline must also be protected online, including the right to privacy. What this means is that actions such as digital surveillance, digital data collection, communication interception, and other forms of cyber espionage must respect the fundamental private rights. Any interference with privacy must meet certain criteria, which are that it must be authorized by unambiguous law, to have a legitimate goal, such as national security or public order, and be proportionate and absolutely necessary to achieve that goal. An arbitrary or widespread surveillance and cyber espionage, particularly one without individualized suspicion, is incompatible with Article 17.[198]

Furthermore, the UN Human Rights Committee's General Comment No. 16 (1988) shed light on the fact that even security measures must not undermine the right to privacy. As such, states must implement effective guarantees against abuse, and any form of digital surveillance must be subject to oversight and precise limits to prevent arbitrary or unlawful intrusions.[199]

In addition, there are other several international instruments that have established some basic principles for data protection in specific. These include the UN Guidelines for the Regulation of Computerized Personal Data Files that were established back in 1990, and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data that were established back in 1980 and then updated in 2013. Both highlight many aspects of data protection including the need for the gathering of personal data to be lawful, transparent, and non-arbitrary, and with the individual's knowledge and consent. It is thus important to note that cyber espionage, by its definition, violates this as is done in secrecy and without people's

---

[197] United Nations General Assembly. (1966). *International Covenant on Civil and Political Rights*. Treaty Series, vol. 999, p. 171. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[198] Office of the United Nations High Commissioner for Human Rights. (2014). *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights* (A/HRC/27/37). United Nations. Retrieved from: https://undocs.org/A/HRC/27/37

[199] UN Human Rights Committee. (1988, April 8). *General comment No. 16: Article 17 (Right to privacy), the right to respect of privacy, family, home and correspondence, and protection of honour and reputation*. Retrieved from: https://www.refworld.org/legal/general/hrc/1988/en/27539

consent. Both instruments are not legally binding as they are considered soft law. However, they reflect some global consensus on minimal data protection standards. In addition, these instruments were used by some states to establish the right to data protection in their domestic laws. [200]

When talking a closer look at Israel's cyber espionage tactics against Palestinians in the West Bank, their tools appear to include extensive and intrusive data collection, which raises serious privacy concerns. That is because Israeli authorities closely monitor millions of Palestinians, through accessing communications such as phone conversations, text messages, social media activity, and even location data, making them "one of the most surveilled people in the world."[201]

The example that was detailed in the previous chapter "Blue Wolf," which aims to take pictures of Palestinians coercively at checkpoints and then compares them to a large database of people's personal information. It must be highlighted that in creating this database, Israeli soldiers competed to capture as many photos as possible of Palestinian men, women, and even children, with rewards given to units that collected the most pictures. Such indiscriminate data collection is the essence of a privacy violation. Palestinians have not consented to being catalogued in an occupying army's "Facebook for Palestinians," and there is no publicly available legal framework governing this surveillance. The practice of omnipresent CCTV monitoring is also another example of how Israel massively collects data on Palestinians.[202]

According to Article 17 of the ICCPR, these interferences are considered unlawful unless Israel can effectively show that they are neither arbitrary nor unlawful. However, there are numerous characteristics that indicate arbitrariness. First, the surveillance used by Israel as a form of cyber espionage is broad in its reach, as it does not only target specific security dangers. Therefore, the indiscriminate mass surveillance of an entire civilian population can be regarded as a disproportionate intrusion on privacy. UN experts have reaffirmed that and emphasized

---

[200] United Nations General Assembly. (1990, December 14). *Guidelines for the regulation of computerized personal data files* (Res. 45/95). Retrieved from: https://www.refworld.org/sites/default/files/legacy-pdf/en/1990-12/3ddcafaac.pdf
Organisation for Economic Co-operation and Development. (2002). *Guidelines on the protection of privacy and transborder flows of personal data* (OECD Privacy Guidelines) . OECD. Retrieved from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2002/02/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_g1gh255f/9789264196391-en.pdf

[201] Institute for Middle East Understanding. (2021, November 29). *Fact sheet: Israeli surveillance & restrictions on Palestinian movement*. Retrieved from: https://imeu.org/article/fact-sheet-israeli-surveillance-restrictions-on-palestinian-movement

[202] See supra note 115.

that indiscriminate mass surveillance fundamentally violates Article 17 because it amounts to an arbitrary or disproportionate measure, even if some security aim is cited, gathering the personal data of countless uninvolved civilians cannot meet the test of necessity and proportionality. Second, the lack of legal openness, transparency, and oversight also contributes to the arbitrariness of Israel's cyber espionage techniques. Military directives and secret processes dominate surveillance in the occupied West Bank, giving Palestinians no effective way to protest data acquisition or seek legal justice. To avoid being "unlawful," human rights jurisprudence states that interferences must be allowed by accessible, specific, and non-retroactive law.[203]

Furthermore, the intrusive nature of the Israeli methods of cyber espionage in the occupied West Bank such as intercepting private phone calls, reading emails or WhatsApp chats, and hacking devices, as it did for instance via Pegasus spyware, which was reportedly found on some Palestinian activists' phones, attacks the essence of "private life" and "correspondence" under Article 17. [204]

It is also important to shed light on the fact that many states including Israel still continuously claim that they do this type of surveillance to deal with security concerns. However, the idea that digital surveillance is acceptable on national security grounds has received many criticisms in literature, particularly when it is in the context of large-scale, unregulated data gathering. Some academics argue in their in-depth analysis of European surveillance regimes that, while intelligence gathering is recognized as a natural function of states, the scale and the purpose of surveillance, particularly when used on people without transparency or oversight, can indeed affect the legality of their uses. They state that national security cannot be used to justify this type of disproportionate or indiscriminate measures that do violate fundamental rights. In such instances, the employment of mass surveillance techniques such as Blue Wolf or Pegasus is invasive, and structurally coercive, which does infringe on private rights that should be guaranteed by Article 17 of the ICCPR.[205]

In addition, the Human Rights Committee's General Comment No. 16 provides a detailed interpretation of the right to privacy under Article 17 of ICCPR. The Committee confirmed

[203] American Civil Liberties Union. (2014). *Privacy rights in the digital age: A proposal for a new General Comment on the right to privacy under Article 17 of the International Covenant on Civil and Political Rights*. https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf
[204] See supra note 192.
[205] See supra note 6.

that this right protects people against both unlawful and arbitrary interference with their privacy, family, home, or more importantly, correspondence. It is important to highlight that even surveillance procedures that are allowed by domestic law could also still be considered violations of Article 17 if they are arbitrary, which means that they are not on rational basis, necessary, or proportionate. The Committee also notes that states have a direct commitment to put in place legal frameworks that would prevent unlawful intrusions. The systemic nature of Israeli cyber espionage against Palestinian civilians, which includes the use of spyware, AI profiling, and metadata surveillance, raise serious concerns about arbitrariness and disproportionality. These actions do not reach the General Comment No. 16 threshold, especially considering the lack of meaningful legal recourse for Palestinians living under occupation.[206]

To further highlight this, in its decision in Toonen v. Australia, the Human Rights Committee expanded on the extent of Article 17 of ICCPR, concluding that any interference with privacy must fulfill strict legality, necessity, and proportionality criteria. The case challenged Tasmania's anti-sodomy legislation, and the Committee concluded that even laws justified by public morality must adhere to international human rights norms. The Committee rejected ambiguous or abstract arguments, emphasizing the fact that the state must show a legitimate need for the intervention and that no less intrusive alternatives exist. This precedent is directly relevant to Israeli cyber espionage methods against Palestinians which Israel claim is for national security. Without clear and personal justification, surveillance tactics such as social media monitoring and mass data collecting, may constitute disproportionate and unjustified invasions into privacy, violating Article 17. The Committee's reasoning in Toonen confirms that security considerations must be thoroughly reviewed and cannot supersede fundamental privacy safeguards, especially when extended to an entire population under occupation.[207]Other cases in international courts have reached similar conclusions.[208]

---

[206] Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy)*, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (1988), para. 3, available at: https://www.refworld.org/legal/general/hrc/1988/en/27539.

[207] See more at: Human Rights Committee. (1994). *Toonen v. Australia*, Communication No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992.

[208]The European Court of Human Rights has also issued major decisions on the legality of monitoring systems in democratic democracies. In Liberty and Others v. United Kingdom (App. No. 58243/00), the Court determined that the UK's legal framework for communication interception lacked sufficient clarity, foreseeability, and oversight, rendering the state's actions incompatible with Article 8 of the European Convention on Human Rights (ECHR), which is similar to ICCPR Article 17. See more at: European Court of Human Rights. (2008). *Liberty and Others v. the United Kingdom*, Application No. 58243/00, Judgment of 1 July 2008.

Therefore, when carefully applying these criteria, Israel's widespread surveillance of Palestinian citizens as a tool for cyber espionage becomes impossible to justify under Article 17. While it is noted that surveillance is not always illegal, states may lawfully monitor suspects for security reasons, but it must be focused and regulated. In the West Bank, however, surveillance appears to be utilized as a general technique of population control, rather than a last-resort tactic against specific dangers. Therefore, the magnitude of targeting Palestinians as a group, imply that the cyber espionage is collective in nature, rather than based on individualized suspicion, which therefore violates the "non-arbitrary" standard. Furthermore, because Palestinians under occupation have no say or representation in the laws and regulations that regulate this surveillance, they are subjected to foreign military surveillance without democratic guarantees, demonstrating arbitrariness and a lack of proportionality. According to Human Rights Committee General Comment 16, even security or anti-crime surveillance must be proportionate and not use the exception to undermine the rule of privacy[209]. Here, it appears that the exception, which is claiming security concerns, has become the norm.

Furthermore, it is important to note that children, as a protected and vulnerable group under international law, are also directly impacted by Israel's cyber espionage practices. Even though IHRL offers specific protections under the Child Right Convention (CRC) and ICCPR, Palestinian children are subjected to invasive surveillance measures, including facial recognition programs like Blue Wolf and routine scanning through CCTV cameras. These practices violate their right to privacy that is particularly articulated in Article 24 of ICCPR that specifies that every child, defined as anybody under the age of 18, "shall have, without any discrimination as to race, colour, sex, language, religion, national or social origin, property or birth, the right to such measures of protection as are required by his status as a minor, on the part of his family, society and the State." [210] This is also articulated in Article 16 "no child shall

On a similar note, In Weber and Saravia v. Germany (App. No. 54934/00), the Court ruled that even mass monitoring for national security objectives must be guided by clear legal regulations, subject to independent oversight, and limited by necessity and proportionality. The Court underscored the importance of protections against abuse, particularly when surveillance is indiscriminate or based on metadata. See more at: European Court of Human Rights. (2006). *Weber and Saravia v. Germany* (dec.), Application No. 54934/00, Decision of 29 June 2006. Retrieved from: https://hudoc.echr.coe.int/eng?i=002-3235
In the context of the Israeli occupation, Palestinians who are subjected to ongoing and intrusive digital surveillance. Israeli methods lack transparency, judicial oversight, and meaningful redress, particularly given the disparity of power and the lack of an effective recourse in Israeli courts. These ECtHR judgments demonstrate that, without strong legislative limits and safeguards, monitoring methods, regardless of their professed purpose, breach fundamental privacy protections under international human rights law.

[209] See supra note 199.

[210] See supra note 192.

be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence." Furthermore, Article 3 of CRC requires that the best interest of the child must be the primary consideration in all actions involving children. [211] Therefore, Israeli intrusive practices also disregard the additional layer of legal protections afforded to children in ways that undermine their dignity and psychological well-being.

In summary, Israel's cyber espionage operations in the occupied West Bank clearly appear to violate the fundamental right to privacy enshrined in Article 17 of the ICCPR. The interception of Palestinians' private communications, homes, and personal data is broad, illegal under any transparent legal framework known to the protected population, and disproportionate to security needs, especially given that civilians are monitored as potential threats. This includes many of the tools it uses like Pegasus, facial recognition systems, mass social media monitoring and surveillance UAVs. This violates the restriction on arbitrary or unreasonable interference. In addition, children's exposure to this type of violation also disregards the additional layer of protection given to children under IHRL. Therefore, Israel's extensive surveillance as a form of cyber espionage in the occupied West Bank lacks consideration for privacy, rendering it incompatible with its international legal obligations.

The right to privacy also has a great impact on other rights like the right to freedom of expression. The next section examines if Israel's cyber espionage against civilians in the West Bank violates the right to freedom of expression and other related rights.

4.2.2 Freedom of Expression and Related Rights

Mass monitoring as a tool of cyber espionage in addition to violating privacy also jeopardizes other fundamental freedoms such as freedom of expression (ICCPR art. 19), peaceful assembly (art. 21), and association (art. 22). These rights are cornerstone liberties under international law, and they remain relevant in the West Bank while occupied.[212] Mass surveillance is known to influence the exercise of these liberties. When people are aware that their communications and general activities are potentially being watched by the occupying authorities, they may self-censor their speech, stop from political activism, or even avoid attending protests, or generally withdraw from civil society groups for fear of any form of repercussions.

[211] United Nations. (1989). *Convention on the Rights of the Child*. United Nations Treaty Series, 1577, 3. Retrieved from: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
[212] See supra note 192.

International human rights experts acknowledge that intrusions into privacy can have a 'chilling effect' on various rights, including the right to free expression. Individuals may be silenced in online communications if they cannot be assured of their privacy.[213]

According to Article 19 of ICCPR, freedom of expression preserves the right to seek, receive, and exchange any type of idea or information. Governments can limit this right in rare, well-defined circumstances, and only when those constraints are lawful, necessary, and proportionate. Israeli methods of cyber espionage could jeopardize this fundamental right in different possible ways. First, Palestinians may avoid discussing certain issues, specifically those in criticism of Israeli policies or support for Palestinian resistance activities, over different communication methods like the phone or online because they are aware that Israeli intelligence monitors social media and telecommunications. As mentioned in the previous chapter, there have been confirmed examples of Palestinians being arrested or interrogated for what they posted online (see section 3.2.1). Israeli authorities frequently charge for "incitement" based on social media activity, incentivizing users to limit themselves and not share their views online or discuss them between themselves.[214]

Such enforcement is enabled because of continuous secretive digital surveillance through different tools that were explained in the previous chapter (see section 3.2.1), and this may violate Article 19 if it is not required to address a real security danger. Often, the broad prosecution of broadly defined "online incitement" suppresses any speech and criticism. This affects both individual expressions and even damages Palestinian public discourse by constantly discouraging free discussion of political complaints or current events.[215]

In addition, several UN bodies have also noted that measures of mass surveillance, specifically when carried out without any clear legal precautions, is a direct threat to the right to freedom of expression that is articulated in Article 19 of the ICCPR. To illustrate, in a UN report back in 2013, the Special Rapporteur on freedom of expression emphasized that both privacy rights and freedom of expression are "interlinked and mutually dependent," emphasizing on the idea

[213] Almutawa, A., & Walker, C. (2024). Chilling effects of surveillance and human rights. *Journal of Human Rights Practice, 16*(1), 397–412. https://doi.org/10.1093/jhuman/huad020

[214] See more at: Chacar, H. (2023, October 20). *Israeli police arrest Arab citizens expressing solidarity with Gaza*. Reuters. Retrieved from: https://www.reuters.com/world/middle-east/israeli-police-crack-down-arab-citizens-expressing-solidarity-with-gaza-2023-10-20/

[215] 7amleh – The Arab Center for the Advancement of Social Media. (2023, December). *Israel's Surveillance Industry and Human Rights*. Retrieved from: https://7amleh.org/storage/Israel%E2%80%99s%20Surveillance%20Industry%20english4.pdf

that excessive intrusion into privacy through the means of surveillance leads to fear, self-censorship, and suppression of political and civic engagement.[216] Following that, various other UN reports emphasized the same points. In 2019 a UN report on Surveillance and Human Rights, also talked about how governments have used different commercial surveillance tools, like those sold by Israel's NSO Group (Pegasus), to target journalists, human rights defenders, and critics, which then often result in arbitrary detention and violations of due process.[217] More recently, in 2024, the UN Office of the High Commissioner for Human Rights reported that Israel has increased monitoring and censorship methods in the Occupied Palestinian Territory to get rid of any form of dissent, discourage civil society participation, and limit freedom of expression.[218] These consecutive reports highlight a consistent manner which is that mass surveillance violates the right to privacy under Article 17, and also directly undermines the exercise of freedom of expression under Article 19.

In the occupied West Bank, Israeli mass surveillance technology, such as the facial recognition systems and AI-driven monitoring, social media monitoring or spywares, have all cumulatively created an atmosphere where Palestinian journalists, activists, and any other regular citizens have been self-censoring out of fear. Palestinians in general are avoiding discussing sensitive matters on digital platforms or communicating with specific sources, preferring in-person discussions to reduce the danger of any type of detection and intrusions. Therefore, even though this type of restraint on freedom of expression is not necessarily overt censorship, it does however successfully limit free expression through creating an environment of psychological pressure where a person feels constantly visible and anticipates punishment for what they may say or share. The cumulative effect is therefore one where individuals stop engaging in open

[216] La Rue, F. (2013). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/23/40). United Nations Human Rights Council. Retrieved from: https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[217] Kaye, D. (2019). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: Surveillance and human rights* (A/HRC/41/35). United Nations Human Rights Council. Retrieved from: https://documents.un.org/doc/undoc/gen/g19/148/76/pdf/g1914876.pdf

[218] United Nations High Commissioner for Human Rights. (2024). *Human rights situation in the Occupied Palestinian Territory, including East Jerusalem, and the obligation to ensure accountability and justice* (A/HRC/55/28). United Nations Human Rights Council. Retrieved from: https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session55/A.HRC.55.28_EN.pdf

communication, not directly because it is legally prohibited, but because of the deeply internalized repercussions of being monitored.[219]

In addition to freedom of expression, the freedom of assembly, enshrined in Article 21 of ICCPR freedom of association, enshrined in Article 22, can also be jeopardized through the same means. For instance, Individuals have the right to peacefully assemble and to organize or join political movements, unions, or any civil society organizations. Despite this, Israeli ways of performing mass digital surveillance against Palestinians have been consistently used to threaten their fundamental rights in the occupied West Bank, which has increased in the aftermath of October 7, 2023. Following this date, there was an increase in the arrests, threats, including tactical restrictions on protests and any kind of public expression of sympathy with Gaza. Israeli security authorities constantly monitor social media platforms like Facebook and WhatsApp for calls to protest or commemorate national events. In several cases, this has resulted in increased military deployments surrounding these planned events, in addition to preemptive arrests of anyone suspected of organizing or attending protests. These methods, that are made possible because of mass surveillance as a form of cyber espionage, prevent peaceful assembly even though it is not done through explicit prohibitions, but it is directly because of creating an environment of fear that discourages collective mobilization and political involvement.[220]

Furthermore, the Human Rights Committee's General Comment No. 37 on the right of assembly also emphasizes that even public assemblies have a component related to privacy. For instance, data-driven identification of protest attendees can violate their privacy and generate “a chilling effect” on participants.[221] Similar to this, the ICRC has also highlighted that "general and indiscriminate surveillance and interference with internet communications – before, during and after – directly interfere with and potentially infringe on freedom of assembly.”[222] In addition, in a report by the UN High Commissioner for Human Rights, it was

[219] France 24. (2024, February 6). *West Bank Palestinians 'exhausted' by omnipresent Israeli surveillance*. France 24. Retrieved from: https://www.france24.com/en/live-news/20240206-west-bank-palestinians-exhausted-by-omnipresent-israeli-surveillance

[220] Mandour, M. (2025, June 18). *Attacks, arrests, threats, censorship: The high risks of reporting the Israel-Hamas war*. Committee to Protect Journalists. Retrieved from: https://cpj.org/2023/10/attacks-arrests-threats-censorship-the-high-risks-of-reporting-the-israel-hamas-war/

[221] United Nations Human Rights Committee. (2020). *General comment No. 37 (2020) on the right of peaceful assembly (article 21)*. CCPR/C/GC/37. Retrieved from: https://docs.un.org/en/CCPR/C/GC/37

[222] Brehm, M. (2020). *Freedom of assembly under attack: General comment No. 37 and interference through surveillance and internet shutdowns*. International Review of the Red Cross, 102(913), 145–170. Retrieved from: https://international-review.icrc.org/articles/freedom-assembly-under-attack-surveillance-interference-internet-communications-913:contentReference[oaicite:3]{index=3}

concluded that there should be prohibition of "the use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising the right of peaceful assembly and association, both in physical spaces and online, and ensure that targeted surveillance measures are authorized only when there is reasonable suspicion that a particular individual has committed or is committing a criminal offence, or is engaged in acts amounting to a specific threat to national security."[223]

In terms of freedom of association, the cyber espionage techniques used by Israeli intelligence targets both persons and groups. Palestinian civil society organizations have long noted that Israel hacks their emails and intercepts office discussions. In 2021, Israel controversially labeled many Palestinian civil rights NGOs as "terrorist organizations" based on what they claim is secret information collected largely through surveillance.[224] This categorization effectively prohibited the work of such organizations and was accompanied by harassment through surveillance means such as tracking worker movements. Therefore, if an entire NGO network is placed under this kind of digital monitoring, as this is not limited to the designated organizations only but contributes to the ongoing shrinking space Israel tries to create to limit Palestinian Civil Society Organizations work as a whole.[225] This may thus lead members to leave, or donors may withdraw, jeopardizing people's right to collectively pursue lawful activities.

Legally, any restriction on the fundamental freedoms of expression, assembly, or association must meet three criteria. It first must be mandated by law. Second, for a legitimate purpose such as national security or public safety, which would entail individualized suspension,

---

[223] Office of the United Nations High Commissioner for Human Rights. (2020). *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests* (A/HRC/44/24). United Nations Human Rights Council. Retrieved from: https://docs.un.org/en/A/HRC/44/24:contentReference[oaicite:3]{index=3}

[224] See more at: Office of the United Nations High Commissioner for Human Rights. (2021, October 26). *UN High Commissioner for Human Rights Bachelet calls Israel's "terrorism" designation an unjustified attack on Palestinian civil society* [Press release]. United Nations. Retrieved from: https://www.un.org/unispal/document/un-high-commissioner-for-human-rights-bachelet-calls-israels-terrorism-designation-an-unjustified-attack-on-palestinian-civil-society-press-release/ and Diakonia International Humanitarian Law Centre. (2021, November 18). *Designation of Palestinian CSOs as "terrorist organisations"*. Diakonia. Retrieved from: https://www.diakonia.se/ihl/news/designation-of-palestinian-csos-as-terrorist-organisations/

[225] See more at: Al-Haq. (2021, November 1). *Designated shrinking space: Israel's systematic harassment of Palestinian civil society organizations* [Briefing paper]. Al-Haq. Retrieved from: https://www.alhaq.org/cached_uploads/download/2021/11/01/briefing-paper-attack-on-palestinian-csos-sp-1635752788.pdf

instead of mass monitoring. Lastly, it should be necessary and proportionate to that purpose[226]. Israel's use of cyber espionage tools to limit fundamental freedoms frequently fails to say the least, on the third point. Extensive mass monitoring of internet speech or gatherings goes beyond what is required to handle specific security concerns, as it classifies almost all Palestinians as possible suspects, which is an unbalanced reaction. Furthermore, the measures are not precisely targeted, meaning that instead of targeting only those Israel claims to be planning violence, they broadly target political critics and demonstration organizers. This broad scope shows that Israel's mass surveillance regime's true purpose is to hold back and get rid of dissent and retain control, rather than simply taking care of genuine dangers. Such an approach violates the requirement that any constraints be the least intrusive manner of accomplishing a reasonable goal.

To summarize, Israel's methods of cyber espionage in the occupied West Bank has a true impact on Palestinian freedoms of expression, assembly, and association. That is because tools like spyware, facial recognition systems, social media monitoring and surveillance UAVs, all create an environment where Palestinians feel the need to self-censor and fear, limiting democratic participation and silencing voices that are very critical to accountability. These fundamental freedoms are protected by IHRL even in the context of occupation, and there are only very limited exceptions allowed. However, it is fair to say that the present Israeli surveillance-based limits are neither narrow nor transparent. They constitute collective suppression of Palestinian political and social activities, which could be a violation of ICCPR articles 19, 21, and 22.

After assessing the right to freedom of expression and other related rights, the next section examines whether Israel's deployment of cyber espionage tools against civilians in the West Bank constitutes a form of discrimination against Palestinians.

4.2.3 Equality and Non-Discrimination

The principle of non-discrimination is one of the foundations and basis of international human rights law. Article 26 of the ICCPR ensures equal legal protection to all people and prohibits

[226] Media Defence. (n.d.). *The right to freedom of expression under international law*. In *Module 1: Key principles of international law and freedom of expression*. Media Defence. Retrieved from: https://www.mediadefence.org/ereader/publications/modules-on-litigating-freedom-of-expression-and-digital-rights-in-south-and-southeast-asia/module-1-key-principles-of-international-law-and-freedom-of-expression/the-right-to-freedom-of-expression-under-international-law/

discrimination in law or practice based on race, religion, or national origin.[227] In the context of an occupation, Article 27 of the Fourth Geneva Convention requires that protected people be treated "with the same consideration" by the occupying power, without adverse distinction.[228] In addition, the Convention on the Elimination of Racial Discrimination (CERD) also prohibits racial discrimination in the exercise of human rights, specifically in Article 5.[229]

Israel's cyber espionage methods in the occupied West Bank could be argued to be biased, as it targets the Palestinian population as a whole. Meanwhile, Jewish Israeli settlers living on the same land, and sometimes in settlements very close to Palestinians, are not subjected to the same extensive secretive surveillance regime. The surveillance system is intended to target Palestinians under occupation. This treatment that could be described as discriminatory is based on nationality or ethnicity and religion. For example, in Hebron's H2 area, where Israeli settlement activity is ongoing and settlers are present daily, Palestinians are the only racial group that are obliged to pass through biometric checks. According to Amnesty's report, "Palestinians are the only racial group of residents in H2 [Hebron] required to use these checkpoints, and the system relies on databases consisting exclusively of Palestinian individuals' data."[230]

Furthermore, the ICJ has also concluded in its 2004 Advisory Opinion that Israel's regime of the broad limitations it imposes on Palestinians violates articles 2(1) and 26 of the ICCPR[231], which are the non-discrimination clauses, as well as articles 2(2) and 3 of the ICESCR[232] and articles 2(1) and 5 of CERD[233]. It is important to highlight that mass secretive surveillance is one aspect of those "comprehensive restrictions," which is a control mechanism that only applies to Palestinians, not Israelis. As Amnesty International has observed that "facial

[227] See supra note 192.
[228] International Committee of the Red Cross. (1949). *Geneva Convention relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention)*. United Nations Treaty Series, vol. 75, p. 287. Retrieved from: https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949
[229] United Nations. (1965). *International Convention on the Elimination of All Forms of Racial Discrimination*. United Nations Treaty Series, vol. 660, p. 195. Retrieved from: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial
[230] See supra note 131, page 6.
[231] See supra note 192.
[232] United Nations. (1966). *International Covenant on Economic, Social and Cultural Rights*. United Nations Treaty Series, vol. 993, p. 3. Retrieved from: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights
[233] See supra note 229.

recognition technology is used extensively by the Israeli authorities to support their continued domination and oppression of Palestinians in the OPT."[234]

To further illustrate, consider the Blue Wolf facial recognition tool and its associated databases, that are exclusively used on Palestinians in the occupied West Bank.[235] Israeli citizens and settlers are not stopped and photographed to be cataloged by Blue Wolf or Red Wolf which were explained in more detail in the previous chapter. On a similar note, Israel's monitoring of phone conversations[236] or social media monitoring conducted by Israel's Unit 8200,[237] are all also limited to Palestinian communications. Israelis living in settlements or even within Israel do not experience such broad intrusive surveillance if there was no specific suspicion in criminal cases. This results in what could be described as a two-tiered Israeli system in which one ethnic-national group, which are the Palestinians, is constantly monitored secretly, while another, which are the Israelis, enjoys privacy and freedom from such intrusions. This distinction is based on national origin and ethnicity, and it is difficult to justify as a security need because it means that millions of Palestinian people are defined by what seems to be group membership. This approach could be argued to be the essence of discrimination.

In accordance with international law principles, not all distinctions are considered unlawful. That is because only discrimination that is not found on reasonable and objective criteria and thus impairs fundamental rights is prohibited. On this basis, Israel regularly argues that the distinction is security-related, for instance to exclude terrorist threats that come from the Palestinian population, not Israelis, therefore that is why the mass surveillance is focused there.[238] However, this Israeli logic is extremely broad and it risks associating the entire civilian

---

[234] See supra note 131, page 8.
[235] See supra note 115.
[236] See more at: Middle East Eye. (2021, November 5). *Israel can monitor every telephone call in West Bank and Gaza, says intelligence source*. Retrieved from: https://www.middleeasteye.net/news/israel-can-monitor-every-telephone-call-west-bank-and-gaza-intelligence-source
[237] See supra note 113.
[238] See the following examples where it is mentioned that Israel reasoning is security related concerns and are needed to identify and track potential threats.
Beaumont, P. (2021, November 5). *Israel escalates surveillance of Palestinians with facial recognition program in West Bank*. The Washington Post. Retrieved from: https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html
Matar, H. (2022, April 27). *Nowhere to hide: The impact of Israel's digital surveillance regime on Palestinians*. Middle East Institute. Retrieved from: https://www.mei.edu/publications/nowhere-hide-impact-israels-digital-surveillance-regime-palestinians
Tufekcioglu, H. (2023, February 15). *Surveillance of Palestinians and the fight for digital rights*. Al-Shabaka.Retrieved from: https://al-shabaka.org/briefs/surveillance-of-palestinians-and-the-fight-for-digital-rights/

population with any prospective threats, resulting in collective punishment (see discussion of collective punishment in Section 3.3.2). Mass, indiscriminate surveillance based on ethnicity or nationality in the absence of any specific suspicion raises severe questions about need, proportionality, and the prohibition of racial discrimination.

Therefore, classifying an entire population as a security suspect class is an example of ethnic or national origin profiling rather than this classification being based on individual behavior. The question here is whether all Palestinians, including children and the elderly, are legitimate targets of this kind of intrusive cyber espionage whereas no Israelis are, simply because of who they are. If the response is yes, then the practice does constitute discrimination. International jurisprudence would require a high level of reasoning for such a broad distinction. The Israeli rationale fails in this case because it presumes guilt or risk through linkage with a certain characteristic which is Palestinian Arab heritage. The Israeli rationale also fails the proportionality criteria. That is because even if the Palestinians could have more security concerns to Israeli authorities, indiscriminately conducting cyber espionage through mass surveillance of all members of that community is not a proportionate security measure when compared to tailored suspect targeting.

On the ground, the prejudice inherent in Israel's cyber espionage system is linked to broader policies that some have labeled as apartheid. In its 2024 Advisory Opinion, the ICJ stated that Israel's policies have resulted in "near-complete separation" of Israeli settlers and Palestinians in the West Bank, violating Article 3 of CERD in addition to Article 26 of ICCPR that prohibits racial segregation.

Mass secretive surveillance emphasizes this division between Palestinians and Israeli settlers in the occupied West Bank by carefully restricting Palestinian movements, activities, and even freedoms whereas settlers move freely without being constantly monitored. It is part of what could be described as an advanced digital control system for a single group. For example, Palestinians must frequently pass through biometric checkpoints, or undergo fingerprint or facial scan, to move between areas within the occupied West Bank, whereas settlers do not. If the right to privacy and free expression are considered human rights, the reality that Palestinians' rights are routinely violated through Israel’s digital monitoring system, but Israeli settlers’ rights are not, is proof of institutionalized discrimination.

Legally, this violates Article 26 of the ICCPR, which ensures equal protection. The ICCPR requires Israel to ensure that no one is denied their rights on discriminatory grounds. However, because of their group identity, Palestinian people in the occupied West Bank are unable to enjoy privacy, freedom of expression, and other basic rights on an equal basis with Israeli settlers living in the same area. The ICJ, in its 2024 Advisory Opinion, criticized this type of dual regime and further noted that this "differentiation of treatment cannot be justified with reference to reasonable and objective criteria nor to a legitimate public aim. Accordingly, the Court is of the view that the régime of comprehensive restrictions imposed by Israel on Palestinians in the Occupied Palestinian Territory constitutes systemic discrimination based on, inter alia, race, religion or ethnic origin."[239]

Furthermore, Article 2 of the ICCPR illustrates that the Covenant's rights should be applied to all individuals within a state's jurisdiction or under their effective control, regardless of race or national origin. Although the occupied West Bank is not part of Israel's sovereign territory, Israel, as the occupying power with effective control over the region, is obliged by human rights duties there.[240] Therefore, Israel, through conducting mass secretive surveillance only on Palestinians in the occupied West Bank and not in Israeli populated areas within the West Bank, Israel fails to secure equal Covenant rights for all under its effective control.

To conclude, the examined cyber espionage techniques mentioned before, that are used by Israel as the occupying power in the occupied West Bank violates peculiar rights like privacy and freedom of expression, but they also violate the fundamental principle of non-discrimination. That is because it targets Palestinians as a whole, without having individual justification for such intrusive secretive surveillance, which portrays Palestinians as inherently suspect. This type of targeting that is collectively based on ethnicity or national origin is directly incompatible with Article 26 of the ICCPR and Israel's duties under CERD. To have any legitimate security concerns, they must be addressed in ways that do not stigmatize or

[239] International Court of Justice. (2024). Advisory opinion on the legal consequences arising from the policies and practices of Israel in the Occupied Palestinian Territory, including East Jerusalem (para. 225). Retrieved from: https://www.icj-cij.org/node/204176. See also paragraphs 196, 205, 213, and 222 for further elaboration on the Court's findings regarding systemic discrimination.

[240] This is articulated in the UN Human Rights Committee, General Comment No. 31 as it says in paragraph 10 that "States Parties are required... to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party." See more at: United Nations Human Rights Committee. (2004). *General comment No. 31: The nature of the general legal obligation imposed on States Parties to the Covenant* (CCPR/C/21/Rev.1/Add.13). Office of the United Nations High Commissioner for Human Rights. Retrieved from: https://www.refworld.org/legal/general/hrc/2004/en/5245

oppress an entire population, otherwise, the measures cross the line into unlawful discrimination.

Thus, after assessing Israel's compliance with non-discrimination principle in relation to its cyber espionage against civilians in the West Bank, the next section looks at if these actions amount to collective punishment under IHL.

4.2.4 Collective Punishment

As discussed in the legal context, even though no active hostilities are now taking place in the occupied West Bank, certain provisions of IHL continue to govern the occupying power's actions in this territory. To be more specific, only the provisions articulated in Article 6 of GCIV continue to apply in the case of prolonged occupation.

For instance, IHL directly prohibits collective punishment and intimidation against protected people. According to Article 33 of the GCIV, "no protected person may be punished for an offense he or she has not personally committed. Collective penalties and likewise all measures of intimidation or of terrorism are prohibited." This provision captures a key principle, which is that accountability is individual, and an occupier cannot penalize or threaten a community for the actions of a few among them.[241]

It is important to highlight that the restriction offered in this provision goes beyond official "penalties" to include "all measures of intimidation", which means any activities that effectively penalize or grow fear for the population as a whole. According to ICRC's Commentary on Article 33, intimidation refers to measures intended to terrorize the population in hopes of preventing hostile acts. These practices are opposed to all principles based on humanity and justice. The Commentary emphasizes that such measures strike at guilty and innocent alike and are prohibited under international humanitarian law.[242] Traditionally, the term collective punishment in the context of actions by Israel against Palestinians, has been used to describe things like retaliation killings, home demolitions of suspect families and closures imposed as retribution.[243] However, the concept of collective punishment should not

[241] See supra note 180.
[242] International Committee of the Red Cross. (1958). Commentary on the Fourth Geneva Convention: Relative to the Protection of Civilian Persons in Time of War. Geneva: International Committee of the Red Cross. Retrieved from: https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-33/commentary/1958
[243] See examples at: Human Rights Watch. (2023, February 2). *Israel: Collective punishment against Palestinians*.Retrieved from: https://www.hrw.org/news/2023/02/02/israel-collective-punishment-against-

be limited to only such activities. It must change to accommodate new technology with similar coercive effects.

When taking a close look at the Israeli cyber surveillance system it applies to Palestinians in the occupied West Bank, Israel seems to surveil everyone in a certain area, or on a broader level, all Palestinians under its effective control, which is both extensive and indiscriminate. Israel collects facial and biometric data from Palestinians in the West Bank as a whole using systems such as Blue Wolf and Red Wolf, usually without individualized suspicion. In addition, after individual security incidents, surveillance is typically noticeably increased in the attacker's town or refugee camp, therefore also affecting those who have no relation to the incident. This is essentially translated to a broad restriction on the population's privacy and freedom, that is imposed on Palestinians under the claim of necessity to prevent the actions of a limited number of individuals alleged to pose a security threat to Israel. However, in reality, millions of Palestinians face a violation of their rights, and an atmosphere of intimidation, not because of their own actions, but because they are part of a population in which some have committed alleged offenses.

These Israeli methods employed create an environment of control and terror amongst civilians, resulting in a system that coerces behavioral conformity not necessarily by force, but through persistent psychological presence. It is important to note that “intimidation” as referred to in Article 33, does not have to only be physical intimidation, it could also be psychological intimidation. There are different studies discussed before in this thesis that show that long-term surveillance causes melancholy, sleep disruption, distrust, and chronic stress. Therefore, intrusive surveillance as a form of cyber espionage against Palestinians in the occupied West Bank may act as a kind of psychological intimidation.

This argument is supported by testimonies from Palestinians who describe how UAVs, locally known as "zanana," fly noisily and visibly above their homes following attacks. H.T., a 36-year-old woman from Nablus, explained that "after any alleged attacks where the Israeli forces claim that the attacker is from Nablus, the first thing we notice is the sound of the surveillance UAVs... It is hard for me and my children to sleep at night because of it. It causes a lot of anxiety, and it just is a constant reminder that we really are always watched.[244]" A.S., a 55-

palestinians , International Court of Justice. (2024). *Advisory Opinion on the Legal Consequences of Israel’s Policies and Practices in the Occupied Palestinian Territory, including East Jerusalem* (para. 212). Retrieved from: https://www.icj-cij.org/sites/default/files/case-related/186/186-20240719-adv-01-00-en.pdf

[244] Interview with H.T., Nablus resident, May 2025. Name anonymized for security reasons.

year-old woman from Jenin, described a similar experience: "Even if we close the windows, it is still very loud. The buzzing sound makes any person very anxious because it is constant... you must live your normal life knowing you are being watched live. It is a horrifying feeling."[245]

Other testimonies highlight the broader geographical and psychological reach of this surveillance. W.S., a 66-year-old man living near the Jenin refugee camp, noted that since early 2025, there has been constant surveillance over the camp and surrounding areas. He stated that he avoids political discussions over the phone due to fear that conversations are being monitored, adding that on several occasions he has heard static and disruptions during calls that made him suspect that the conversation is being heard by a third party.[246] Furthermore, M.A., a 19-year-old man from Ramallah, added that the sound of the surveillance UAVs gives him “major headaches and anxiety. It just makes me feel uncomfortably watched... We become very scared to openly communicate on our phones."[247] Similarly, R.T., a 33-year-old woman from Hebron, described the intensified surveillance in the aftermath of an attack allegedly committed by a resident of the city: "Of course we faced city closures, daily incursions, and also increased surveillance against all of Hebron’s residents. The zanana makes me feel frustrated... sometimes unable to focus."[248]

Thus, these testimonials do reveal a clear pattern, which is that the Israeli use of mass intrusive cyber surveillance are not surgically or proportional use, because they target the entire community which is also unpredictable in duration.[249]

Therefore, Israeli cyber espionage has the capability to intimidate large groups of Palestinians. Knowing that the entire community is being tracked, with the constant message of “we are watching you all,” is a common message used to discourage potential attackers However, it also terrorizes ordinary citizens who have no intention of conducting any attacks. The broad scope of surveillance results in collective psychological punishment, which is the loss of any sense of privacy.

---

[245] Interview with A.S., Jenin resident, May 2025. Name anonymized for security reasons.
[246] Interview with W.S., Jenin resident, May 2025. Testimony provided in Arabic and translated by the author.
[247] Interview with M.A., Ramallah resident, May 2025. Name anonymized for security reasons.
[248] Interview with R.T., Ramallah resident, May 2025. Name anonymized for security reasons.
[249] These testimonies were collected by the author in May 2025 from residents of Nablus, Jenin, Hebron, and Ramallah. All names have been anonymized for safety. Interviews were conducted verbally and translated by the author from Arabic where applicable.

In accordance with Article 33, such intimidation is prohibited. The logic is that innocent civilians should not suffer to discourage offenders. Even if Israeli surveillance is officially justified as a means of deterring terrorism, it cannot be ignored that it entraps innocent people who are forced to give up their liberty and sense of security. This does match the definition of a collective punishment, which terrorizes an entire community.

It is worth emphasizing that mass surveillance as a tool for cyber espionage can be interpreted as a type of collective punishment for rights. It is not a typical "penalty" in the sense of detention or fine, but rather a human rights penalty inflicted collectively on privacy, and expression.

Moreover, Article 33 also forbids "measures of terrorism." The "terrorism" in this context refers to acts that are intended to implant fear in the civilians. Even though the term came before modern usage, it can still be argued that it essentially encompasses cyber intimidation tactics. Therefore, it could be argued that constantly making an entire population live in fear and that every move is being watched and could be used against them could then constitute spreading terror or fear among civilians.

Therefore, in these circumstances, the cumulative effect of increasing the amount of intrusive surveillance, like longer drone presence, in addition to other factors like movement restrictions imposed at such situations, particularly when triggered by the actions of a single individual, gives the impression that all people of the targeted region are alleged to be suspects. Typically, Israel could give the claim that these methods are done to ensure security. However, the indiscriminate application of these methods could show a system of punishment and control that is directed at the entire area. Which is why this seems questionable when looking at the fundamental IHL principle that accountability is individual and cannot be generalized. This technique also conveys a clear coercive message, that the entire community will be monitored, contained, and penalized for the activities of one or a few individuals. Such an approach is consistent with the idea of collective punishment outlawed by Article 33 of the Fourth Geneva Convention. As one resident of Hebron, R.T., put it, “as soon as we see where the attacker is from, we know that area will be under hell.”[250]

[250] See supra note 253. Interview with R.T., Ramallah resident, May 2025. Name anonymized for security reasons.

It is also very important to note that there is no treaty body or court that has yet declared widespread monitoring as a form of cyber espionage as a form of collective punishment. However, this thesis argues that its logic, extent, and consequences are consistent with previously acknowledged violations of Article 33. This is especially seen when surveillance is 1) indiscriminate, as it is used to target Palestinians as a whole rather than specific individuals, 2) seems punitive in its intent, as it increases after attacks, 3) Seems to be used for psychological intimidation, and 4) disproportionate to the actual threat. The argument is that just as home demolitions harm innocent family members, digital surveillance affects every resident of a specific monitored region, which directly invades their right to privacy and also puts at risk their psychological well-being. As a result, this thesis attempts here to contribute to an evolving legal discourse by arguing that cyber monitoring should be evaluated not only for data protection concerns, but also as a potential means of collective punishment under IHL.

Thus, after examining the specific legal concerns that arise due to the act of cyber espionage itself, the next section looks at a different angle which is the legality of the use of information that is derived from the act of cyber espionage. This is important because the legality of using information obtained through unlawful means raises distinct legal questions.

4.3 Legal Considerations Regarding the Use of Cyber Espionage Derived Information

When evaluating the legality of Israel's cyber espionage methods it uses in the occupied West Bank, it is critical to look at the means of data collecting but also the purposes for which such data is eventually used. Israeli cyber surveillance does not exist in a vacuum. The intelligence obtained through cyber espionage can, and usually is, used in further actions with direct legal complications under both IHRL and IHL. Coercive tactics include informant recruitment, arrests based on predictive digital profiling, and, in some circumstances, the use of fatal force. Therefore, this section examines how the legality of the use of cyber espionage derives information.

4.4.1 Arrest and Detention Based on Digital Profiling

Article 9 of the ICCPR articulates the right to liberty and the security of a person, and it gives guarantees that no one should be arbitrarily arrested or detained. The article notes that if a

person's liberty shall be taken, then it must be in complete compliance with the established law, it also must be based on legal grounds and processes that are not arbitrary or discriminatory and have clear judicial oversight.[251]

When the context of the Israeli operations in the occupied West Bank is closely looked at, the arrests and detentions of Palestinians could usually be a result of surveillance data gathered coercively. This means that the intelligence that is gathered by cyber espionage like social media monitoring, communication interference, or even location tracking through means like surveillance UAVs, can lead to Israel identifying individuals as suspects and then arrest them. Here, a major question arises on whether these arrests are "arbitrary" under Article 9.

In this context, there are several patterns that can be seen. Firstly, according to reports, Israeli security personnels use algorithms to identify Palestinians who may represent a security concern based on their internet activity patterns, known as "predictive policing". The detailed examples of how Israel uses this to arrest Palestinians based on their social media posts can be found in the previous chapter (see section 3.2.1).[252] Based on that, if individuals are to be held based on large data obtained or on misconstrued posts, then this could be seen as arbitrary. That is because these methods lack transparency and can easily trap innocent people or those exercising protected freedom of expression. Clearly, an arrest that occurs without a sufficient evidentiary foundation, made because an algorithm pointed someone as "suspicious," fails the criterion of rationality and necessity required to avoid arbitrariness.

Secondly, exclusively in the occupied West Bank, Israel uses administrative detention, which is the imprisonment of individuals without a proper list of accusations, typically based on secret evidence. According to latest counts by the Palestinian Commission of Detainees and Ex-Detainees Affairs, there are 3,577 Palestinians in administrative detention, the largest number in decades.[253] Many of these detentions are likely based on digital intelligence as part of a secret file provided to military courts to legitimize the detention. The detainee and their lawyer are unable to see the evidence which limits their ability to challenge it. Arresting and holding someone indefinitely because of an intelligence dossier, perhaps based on cyber espionage that

[251] See supra note 192.
[252] See supra notes 136 and 138.
[253] Commission of Detainees and Ex-Detainees Affairs. (n.d.). *Official website*. Retrieved May 26, 2025, from: https://www.cda.gov.ps/

alleges they are implicated in future crimes or belong to a banned group is extremely problematic under Article 9.[254]

Recent official reports have expressed deep concern about Israel's increasing use of administrative detention against Palestinians. They describe this as incompatible with Article 9.[255] According to the Addameer Prisoner Support and Human Rights Association, the secret evidence they refer to is usually gathered from intelligence sources. Therefore, this could also violate Article 14 of ICCPR which talks about the need to have due process.[256]This presents the true likelihood that data obtained through cyber surveillance and digital espionage is being used to support these detentions.[257]

Thirdly, covert surveillance may identify someone based on their political or social profile, rather than their actual crime. If those individuals are arrested "preemptively" or on false accusations to remove them from the situation, then their arrests are used as an instrument of repression rather than law enforcement. Arbitrary detention also includes detaining individuals based on their protected rights or without a strong legal basis for the arrest, as asserted in the UN Human Rights Committee's General Comment No. 35.[258] There have been many instances where Israel did that. For instance, during the May 2021 protests, in which Israeli forces used digital tracking to locate and round up protest organizers and participants in large numbers. Amnesty International documented discriminatory arrests of Palestinians in East Jerusalem and Israel by using digital monitoring and facial recognition tools to identify protestors, many of

---

[254] See more at: Gunter, J. (2023, December 15). *How Israel jails hundreds of Palestinians without charge*. BBC News. Retrieved from: https://www.bbc.com/news/world-middle-east-67600015

[255] See more at: United Nations Office of the High Commissioner for Human Rights. (2024, July 31). *UN report: Palestinian detainees held arbitrarily and secretly subjected to torture by Israeli authorities*. Retrieved from: https://www.ohchr.org/en/press-releases/2024/07/un-report-palestinian-detainees-held-arbitrarily-and-secretly-subjected , Amnesty International. (2023, November 8). *Israel/OPT: Horrifying cases of torture and degrading treatment of Palestinian detainees amid spike in arbitrary arrests*. Retrieved from: https://www.amnesty.org/en/latest/news/2023/11/israel-opt-horrifying-cases-of-torture-and-degrading-treatment-of-palestinian-detainees-amid-spike-in-arbitrary-arrests/ and Human Rights Watch. (2023, November 29). *Why does Israel have so many Palestinians in detention and available for a swap?* Retrieved from: https://www.hrw.org/news/2023/11/29/why-does-israel-have-so-many-palestinians-detention-and-available-swap

[256] See supra note 192.

[257] Addameer Prisoner Support and Human Rights Association. (2016, July). *Administrative detention in the occupied Palestinian territory: A legal analysis report*. Retrieved from: https://www.addameer.org/sites/default/files/publications/administrative_detention_analysis_report_2016.pdf

[258] United Nations Human Rights Committee. (2014). *General Comment No. 35: Article 9 (Liberty and security of person)*, CCPR/C/GC/35, paras. 12, 17.Retrieved from: https://undocs.org/CCPR/C/GC/35

whom were then detained without proper cause or accusation. Therefore, this kind of usage is arbitrary and breaches both Article 9's promise and Articles 21/22, as previously established.[259]

To further explain, a former Unit 8200 Israeli soldier exposed the cyber espionage tactics employed by Israel in general and how they gather digital information and arrest based on that. He notes that "The Palestinian population under military rule is completely exposed to espionage and surveillance by Israeli intelligence ... .in many cases, intelligence prevents defendants from receiving a fair trial in military courts, as the evidence against them is not revealed."[260]

Thus, having due process is very essential. Article 9(2) specifically notes that anybody detained must be told the reason behind the arrest and given a list of charges behind the arrest.[261] When Palestinians are arrested because of secret surveillance gathered by Israeli intelligence, they are usually not informed of the true reason and instead are given a broad explanation of "security reasons".[262] In addition, Article 9(4) provides the right to appeal the detention in court. However, in these "security situations," Israeli military courts commonly defer to secret evidence, which makes the ability to challenge the arrest very difficult without knowing what the arrest was for. General Comment No. 35, referred to earlier, also notes that detention because of national security must be exceptional. In addition, in this case, the state must show their necessity and proportionality. The General Comment also emphasizes that individuals must be informed of the reasons for their imprisonment and given the right to challenge it before a court.[263] However, Israel's use of cyber espionage techniques as part of its intelligence, in the occupied West Bank, where persons are frequently detained based on secret data or algorithmic profiling, lacks these procedural protections, which seems to violate Article 9.

Moreover, under IHL in occupation law, extended detention without trial may violate GCIV prohibitions. For example, Article 78 allows detention only for "imperative security reasons"

---

[259] Amnesty International. (2021, June 24). *Israeli police targeted Palestinians with discriminatory arrests, torture and unlawful force*. Retreieved from: https://www.amnesty.org/en/latest/press-release/2021/06/israeli-police-targeted-palestinians-with-discriminatory-arrests-torture-and-unlawful-force/

[260] See supra note 144.

[261] See supra note 192.

[262] Gunter, J. (2023, December 15). How Israel jails hundreds of Palestinians without charge. BBC News Pidgin. Retrieved from: https://www.bbc.com/news/world-middle-east-67600015

[263] United Nations Human Rights Committee. (2014). *General Comment No. 35: Article 9 (Liberty and security of person)*, CCPR/C/GC/35, paras. 12, 17.

and with procedural guarantees. Therefore, when digital profiling loosely labels people as risks and then they are arrested accordingly, it does not meet the "imperative" standard.[264]

Therefore, when many Palestinians are arrested and detained in unclear processes based on data gathered by secret covert surveillance intelligence, this violates Article 9 and related fair trial rights described in Article 14. In conclusion, the covert surveillance-based arrests and detentions in the occupied West Bank regularly violate international standards. They usually qualify as arbitrary arrests. That is because they do not have the legal basis needed, they are disproportionate, or are based on discriminatory targeting, which therefore violates ICCPR Article 9.

Thus, after having illustrated the illegality of using cyber espionage to arrest civilians, the next section examines the legality of using cyber espionage derived information for coercion and recruiting informants.

4.3.2 Coercion and Informant Recruitment

In the GCIV, precisely in Article 31, the issue of coercion to seek information is stated. The article notes that "no physical or moral coercion shall be exercised against protected persons, in particular to obtain information from them or from third parties."[265] Therefore, the GCIV clearly prohibits forcing individuals to provide information, including those where the goal is to gather intelligence. It conveys the fundamental principle that an occupying power cannot force the occupied people to cooperate or collaborate against their will. Therefore, the occupation law emphasizes that civilians cannot be required to help the occupier's security activities, except in fundamental requirements such as adhering to security laws, and they cannot be pressured into spying or informing.

The relationship between Article 31 and Israeli cyber espionage techniques to gather intelligence is clear. That is, the information taken from such digital covert methods can then be used to exert pressure on individuals to become informants. Therefore, some surveillance-derived information can be used for coercion and blackmail by Israel. There have been documented cases where testimonies from Palestinians show that Israel's security agencies, especially Unit 8200 that was discussed in detail in previous chapters, have engaged in such

[264] See supra note 180.
[265] *Ibid.*

abuses in the occupied West Bank. An example to this is the targeting of queer Palestinians, through cyber espionage tools and threatening exposure of their sexual orientation, that was detailed in the previous chapter (see section 3.2.1).

Therefore, such uses are clear violations of GCIV Article 31. What is important to note is that Article 31 does not make a distinction between physical coercion, like beatings, and "moral coercion," which includes this kind of psychological pressure, and making threats to one's family, and social stigma, they all are equally illegal. The phrase in the article "in particular to obtain information" is very significant. That is because occupiers have historically tried to coerce civilians into providing military information, like revealing the location of resistance fighters, which is expressly prohibited by the Geneva Convention. More recently and in the digital era this has also evolved into incorporating the technological means to coerce or blackmail civilians. Therefore, Israel's use of cyber espionage techniques to identify someone's secret and very personal information, not only violating their privacy, but then threatening to expose that secret unless they become informants for Israel is a clear example of moral coercion. What is also important to note is that Article 31 violations might be considered grave breaches if the coercion is extreme. Even without that, it is a significant violation of IHL.

On this note, Israel may argue that people give information voluntarily or that cooperating with intelligence is optional. However, it is also important to acknowledge the documented threats that are made by Israeli intelligence officers if the person refuses to cooperate. Therefore, in this context volunteering" is often a fabrication. In addition, the occupation is inherently coercive, and there is a power disparity between the occupier and the occupied that makes any apparent consent compromised on different levels.

Furthermore, it is very important to highlight that coercion into becoming an informant is dangerous. Protected persons under occupation, as detailed in Article 4 of the GCIV, are meant to remain outside of hostilities[266]. Even though the protection is not automatically lost because of coercion, forcing a civilian to act as an informant or spy risks blurring the line between civilian and participant in hostilities, which may jeopardize their safety and perceived neutrality. In this way, the occupying power seems to take advantage of the civilian's protected status, but while also diminishing and risking it. This then creates a self-serving method for the

[266] See supra note 180.

occupier, in which it does not take into account its legal commitment to protect civilians as articulated in Article 27 of the GCIV[267], in order to achieve its own intelligence goals.

Finally, the use of the cyber espionage derived information by Israel through examined methods detailed earlier, to coerce and blackmail Palestinian in the occupied West Bank to become informants is a grave breach of Article 31 of the GCIV.

Thus, after concluding that the use of cyber espionage derived information for coercion and recruiting informants, the next section looks at how the information taken can lead to more fatal actions in the West Bank such as targeted killings.

4.3.3 Targeted Killings and Lethal Operations

As enshrined in IHRL, particularly in Article 6 of ICCPR, the right to life is the most fundamental human right that prohibits the arbitrary deprivation of life. Therefore, states must abide by very strict requirements even in security operations.[268] In law enforcement contexts, these strict requirements are that lethal force can only be used when essential to defend life. On the other hand, in armed conflicts, states must also comply with the limitations set out by IHL, which are distinction, proportionality, and military necessity. Therefore, as the occupied West Bank is not considered a place where active hostilities exist under IHL, this means that operations there must conform to the law enforcement paradigm under IHRL. This means that any deliberate use of fatal force must be strictly necessary and proportionate to an immediate threat.[269] Therefore, extrajudicial killings are clearly prohibited by IHRL, as it is considered a grave violation of Article 6, and by IHL, as it would define these willful killing of a protected person under Article 147 of GGIV[270].

Cyber espionage can also help the use of force by giving intelligence on targets' locations and activities. In recent years, the Israeli military has been committing what seems to be "targeted killings" in the West Bank. Targeted killings refer to the intentional and pre-meditated use of

[267] *Ibid.*
[268] See supra note 192.
[269] See more at: Diamond, E., Nohle, E., & Schmidl, A.-C. (2025, January 30). *The legal framework regulating Israel's use of force in the West Bank*. Opinio Juris. Retrieved from: https://opiniojuris.org/2025/01/30/the-legal-framework-regulating-israels-use-of-force-in-the-west-bank/
[270] See supra note 180.

lethal force, by a State or organized armed group against a specific individual outside their physical custody.[271]

Up until recently, the Israeli military initially used drones for surveillance in the West Bank, as there were not recorded lethal drone strikes between 2006 and 2023, as this method was effective for operations in Gaza. In June 2023 however, Israel conducted a drone attack on the Jalamah area in Jenin, which killed three alleged Palestinian militants. That attack was the first one in the West Bank in nearly two decades showing that there has been a real shift in the Israeli military's tactics. Since that, drone strikes have been more common in the occupied West Bank.[272] By 2025, these attacks had become a component of military incursions, especially in heavily populated refugee camps like Jenin. What is important to note is that these operations on a typical basis combine drone surveillance, precise missile strikes, and ground raids, resembling the integrated military approach used in Gaza.

These Israeli drone strikes have been showing patterns that indicate the use of surveillance capabilities as a form of cyber espionage in these targeting operations. To give a recent example, in February 2025, a drone attack in Jenin killed a 14-year-old child, and injuring two others. In this case, the child, Ahmad, was sitting in his backyard waiting for his relative, Nour, to come visit when the drone strike hit and took his life. Nour was known to be wanted by the Israeli authorities. According to documentation by Defense for Children International, Palestine (DCIP), Nour, was near Ahmad's home, but survived the first strike. However, he was targeted by another Israeli drone, which killed him in addition to a Palestinian nurse who was working in the area.[273] This example raises severe issues regarding the combination of cyber espionage with targeted operations. It appears that Israeli intelligence tracked Nour, possibly using cyber espionage tools like phone information or surveillance UAVs and attempted to target him with a drone strike in a civilian neighborhood. The failure of the first strike, followed by a second, more lethal one, shows a targeting strategy based on live intelligence inputs and possibly modified by real-time data collection.

[271] International Committee of the Red Cross (ICRC). (n.d.). Targeted killings. ICRC Casebook. Retrieved from: https://casebook.icrc.org/a_to_z/glossary/targeted-killings
[272] Gritten, D. (2023, June 22). *Rare Israeli drone strike kills Palestinian militants in West Bank*. BBC News. Retrieved from: https://www.bbc.com/news/world-middle-east-65984374
[273] Defense for Children–International Palestine. (2025, February 3). Israeli drone strike kills 14-year-old Palestinian boy in Jenin. Defense for Children Palestine. Retrieved from: https://www.dci-palestine.org/israeli_drone_strike_kills_14_year_old_palestinian_boy_in_jenin

The legal discussion that arises here is when cyber espionage derived intelligence is used to conduct these kinds of targeted lethal operations in situations where lethal force is not allowed under international law. Outside active hostilities, security forces must try to arrest the needed target and may only use lethal force if the suspect poses a threat of death or serious injury and no other options, such as capture are available. However, many of these drone strikes in the West Bank take place in densely populated civilian areas meaning that the strike has a high chance of also targeting other civilians, such as children, like in the example indicated above. In addition, even the targeted people are not actively involved in hostilities at the time of this type of strike, which raises the legal questions of whether using force to execute them is allowed. It is very important to note here that even militants in the West Bank are not considered combatants under international law and are still civilians.[274] In such cases, where the target poses no immediate threat and no arrests are pursued, these operations may constitute extrajudicial killings, violating both international human rights law and occupying power's legal obligations.

It is also important to highlight that this kind of targeted killing can also happen in other ways, not just in drone attacks, and still have proven that it was due to real time surveillance. For instance, in March 2022, Israeli soldiers killed three Palestinians in Nablus in a car after supposedly tracking them, perhaps by phone surveillance, or surveillance UAVs.[275] No warning or effort to arrest was made, which experts claimed could amount to extrajudicial killing.[276] If cyber info is used to locate someone and then they are executed without being given the opportunity to surrender, both the right to life and due process are violated.

Thus, when examining Article 6 of the ICCPR, it states that the denial of life cannot be arbitrary, meaning that it cannot be unjust, unlawful, and unnecessary killings. A targeted killing can be arbitrary when it is not properly used as the very last resort, and when there is a lack of clear transparency and oversight. The use of drones or commandos to kill persons identified by surveillance raises questions about accountability. Usually, the justification is not

[274] This was also emphasized by the Israeli Supreme Court ruling in 2006. See more at: Public Committee Against Torture in Israel v. Government of Israel, HCJ 769/02 (2006). Supreme Court of Israel.
[275] Al Jazeera. (2022, February 8). *Israeli soldiers open fire at car in Nablus killing Palestinians*. Retrieved from: https://www.aljazeera.com/news/2022/2/8/israel-troops-kill-three-palestinians-in-occupied-west-bank
[276] See more at: Al-Haq. (2022, March 3). *Urgent Appeal to the United Nations Special Procedures on the Extrajudicial Execution and Wilful Killing of Palestinians Mr. Ashraf Mubaslat, Mr. Mohammad Dakhil, and Mr. Adham Mabrukah, by the Israeli Occupying Forces on 8 February 2022 in Nablus, West Bank*. Retrieved from: https://www.alhaq.org/cached_uploads/download/2022/03/13/urgent-appeal-extra-judicial-killings-nablus-1647198805.pdf

fully disclosed, as the claim is that it is due to security reasons, which could amount to a violation of Article 6 which also includes the right to an effective examination of any deprivation of life.

What is also very import to note is that the Israeli Supreme Court in 2006 on targeted killings, acknowledged in its decision that, while there may be exceptional cases in non-traditional conflicts where targeting a militant is permissible, each case must be examined closely, and if capture is possible, it should be attempted rather than killed.[277] However, it is not very clear that Israel does meet this threshold because multiple incidents indicate fatal force being used when suspects were in a situation where potentially non-lethal tactics could have been used.

In addition to that, when surveillance data is used to conduct drone strikes, as have been suspected occasionally in the occupied West Bank, there is an additional risk of misidentification. Surveillance can sometimes lead to false positives, killing the wrong person based on faulty data, as has also happened in other conflict theatres.[278] Any such mistake in the West Bank would be an arbitrary deprivation of life.

Looking at the context from a human rights perspective, every use of lethal force by Israeli forces in the occupied West Bank must be very specifically assessed for necessity. According to Human Rights Watch 2024 report, killings of Palestinians in the West Bank reached a very high number with many of them being illegal.[279] This then shows how there is a tendency in which rules of engagement have loosened, therefore treating the West Bank like an active war zone, especially following October 7, 2023.[280] Cyber espionage methods that Israel has and uses increases its ability to neutralize special targets, and that does not alter the legal constraints in which if it is possible to arrest rather than kill, or if the person does not pose an imminent threat, killing them is prohibited.

---

[277] Israeli Supreme Court. (2006, December 14). *Public Committee Against Torture in Israel v. Government of Israel* (HCJ 769/02). Retrieved from: https://versa.cardozo.yu.edu/sites/default/files/upload/opinions/Public%20Committee%20Against%20Torture%20in%20Israel%20v.%20Government%20of%20Israel.pdf

[278] See example at: Hennigan, W. J. (2021, September 17). *'A Tragic Mistake.' Botched Drone Strike in Afghanistan Raises Concerns Over Biden's Counterterrorism Strategy*. Time. Retrieved from: https://time.com/6099377/afghanistan-drone-strike-counterterrorism/

[279] Human Rights Watch. (2024, May 8). *West Bank: Israeli Forces' Unlawful Killings of Palestinians*. Retrieved from: https://www.hrw.org/news/2024/05/08/west-bank-israeli-forces-unlawful-killings-palestinians

[280] See more at: Human Rights Watch. (2024). *Israel and Palestine*. In *World Report 2024*. Retrieved from: https://www.hrw.org/world-report/2024/country-chapters/israel-and-palestine

In addition to the conclusion that information derived from cyber espionage can lead to targeted killings in the West Bank, which violates the right to life under IHRL, such practices could also violate the fundamental right to due process. Under Article 14 of the ICCPR, individuals have the right to a fair trial and the presumption of innocence when accused of a crime. However, in the context of the West Bank, Israel's practice of identifying and killing people through surveillance is equivalent to carrying out the punishment of death without any legal process, therefore completely disregarding the rule of law. This resembles a "death penalty without trial," that Special Rapporteur Philip Alston once described certain U.S. drone strikes as analogous to judges, juries, and executioners rolled into one, and the same critique applies here.[281]

The right to due process under IHRL is not limited to formal judicial processes, as it also applies to every situation in which the state uses coercive authority against individuals. When surveillance data is used to carry out extrajudicial killings without notice, arrest, or the opportunity to refute claims, it violates procedural protections that are fundamental to both the right to life and the administration of justice.[282]

As a result, the use of digital secretive surveillance data to assist targeted executions in the West Bank raises major legal concerns under Article 6 of ICCPR. Many such operations risk being classified as extrajudicial killings because they bypass the court process and frequently fail to meet the conditions for deploying lethal force. The accountability gap is considerable. Israeli investigations into such killings are rare, which shows a culture of impunity that Article 6(1), read with the duty to preserve life, prohibits.[283] In its General Comment 36 on the right to life, the Human Rights Committee emphasized the importance of states investigating and accounting for any possibly wrongful deprivation of life.[284] In the West Bank, intelligence-based killings are frequently dealt with in secrecy claiming it is a "security operation" which leaves Palestinians with no justice. This is a violation of the right to life's protective regime. In

[281] Peacekeeping and Stability Operations Institute. (2020). Drone case study. U.S. Army War College.
[282] Rishmawi, M. (2019, November). Protecting the right to life in protracted conflicts: The existence and dignity dimensions of General Comment 36. International Review of the Red Cross, 101(912), 1149–1169. https://doi.org/10.1017/S1816383120000272
[283] See more at: B'Tselem & Palestinian Centre for Human Rights. (2021, December). *Unwilling and Unable: Israel's Whitewashed Investigations of the Great March of Return Protests*. Retrieved from: https://www.btselem.org/sites/default/files/publications/202112_unwilling_and_unable_eng.pdf
[284] United Nations Human Rights Committee. (2018, October 30). *General comment No. 36 on article 6 of the International Covenant on Civil and Political Rights, on the right to life* (CCPR/C/GC/36), paras. 27–29. Retrieved from: https://docs.un.org/en/CCPR/C/GC/36

addition, this is also a violation of the right to due process articulated in Article 14 of the ICCPR as Israel kills individuals without offering them the right to go through a fair trial.

Therefore, while cyber surveillance is allegedly intended to improve security, its use to take part in fatal operations in the occupied West Bank frequently conflicts with Israel's commitment to protect life and use force only when absolutely required.

To conclude the entire chapter, there has been an investigation into the legal consequences of the Israeli cyber espionage methods against the Palestinian people in the occupied West Bank. On that basis, many legal questions arose incorporating both IHRL and IHL, regarding both the act of cyber espionage itself and the use of the information it gathers. On the level of cyber surveillance Israel conducts as a form of cyber espionage, Israel's extensive monitoring and data collection violates the essential rights of the occupied population. The listening in of private communications, facial recognition tracking, and bulk data mining of personal information through the examined Israeli tools all violate the right to privacy articulated in Article 17 of the ICCPR, in an arbitrary and excessive way. In addition, as children are also impacted, it also violated the additional protection offered to them in both ICCPR and CRC. The Israeli cyber espionage methods also violate Palestinians' rights to expression, assembly, and association because they create fear and self-censorship in the West Bank. Cyber espionage is also used in a discriminatory way, as it mainly targets Palestinians due to their identification, which thus breaks the principle of equal protection granted in Article 26 of ICCPR and also amounts to systemic ethnic discrimination, as observed by ICJ. Children are also not exempt from these acts, which violate the specific protections they need as articulated in CRC and ICCPR. From an IHL perspective, the cyber espionage system Israel also do not directly comply with the prohibition to using means of intimidation against the civilian population as articulated in Article 33 of GCIV, because the always present surveillance aims to intimidate and control the population.

In terms of the use of cyber espionage derived information, this chapter focused on contexts in which Israel uses obtained intelligence to more complex legal violations. Therefore, the chapter focused on the issues of arbitrary arrests, which is a violation to Article 9 of ICCPR, and coercion by Israel to blackmail Palestinians to become informants, which violates Article 31 of the GGIV, and the enabling of targeted killings which violates Article 6 of ICCPR.

Even though this chapter has focused primarily on Israel's obligations under IHRL, given the law enforcement nature of its conduct in the West Bank, it is important to highlight that IHL also continues to apply, even if partially, because of the occupation. The analysis of collective punishment under IHL highlights just one aspect of broader concerns. Taken together, the evidence suggests that Israel's cyber espionage practices against civilians in the West Bank violates core principles of privacy, freedom of expression, and non-discrimination under IHRL and the prohibition of collective under IHL also seems to not be met.

These cyber espionage methods are not only used against civilians in the West Bank, as they are also used against them in the Gaza Strip. Thus, the next chapter addresses the context in Gaza, which is under a more explicit hostilities paradigm, a comparative perspective will emerge.

Chapter Five: Cyber Espionage and Military Targeting in Gaza

As the previous chapter looked at Israeli cyber espionage against civilians in the occupied West Bank within a law enforcement framework governed mainly by IHRL and then, IHL, this chapter shifts the focus on the Gaza Strip, where the Israeli cyber espionage technologies are used in a context of active hostilities. However, given the intensity and character of the active hostilities, especially since October 7, 2023, this chapter focuses on IHL as the *lex specialis* controlling hostilities. It examines whether Israel's use of cyber espionage tools in Gaza is consistent with important IHL core principles of distinction, proportionality, and precaution. In addition, where applicable, the chapter outlines specific violations of important IHRL standards, particularly the right to life, to emphasize the complementarity of both bodies of law.

5.1 Legal Framework

To properly analyze the legality of cyber espionage as a technique for military targeting in Gaza, the applicable legal frameworks governing the region must first be clarified, as it differs from the West Bank. In addition to looking at the relevant frameworks, this section also looks at how Israel's cyber espionage technologies have become an essential tool to Israeli military operations in Gaza. Therefore, this section provides the legal and operational or practical frameworks for evaluating the legality of the use of cyber espionage in Gaza.

5.1.1 Applicable Legal Frameworks in the Gaza Strip

The Gaza Strip has a complex legal framework for the application of both IHL and IHRL. First, the question of whether Gaza is still considered an occupied territory after Israel's disengagement in 2005 is an important place to start the discussion. The Israeli government claims until this day that it ended its occupation of Gaza in 2005, as it withdrew its forces from the ground and evacuated its settlements, therefore giving up "effective control" over Gaza[285]. Officials in Israel say that because they have no permanent military presence in Gaza, that effectively means that they no longer occupy the Strip and therefore they are no longer subject

[285] See more about Israel's 2005 disengagement: Stead, R. (2019, August 15). *Remembering Israel's 'disengagement' from Gaza*. Middle East Monitor. Retrieved from: https://www.middleeastmonitor.com/20190815-remembering-israels-disengagement-from-gaza/

to the occupying power duties articulated in GCIV. [286]However, this viewpoint is debunked internationally. The ICRC,[287] the UN,[288] the ICC,[289] international NGOs[290] and several legal experts all assert that Israel's rule over Gaza did not terminate in 2005 and that it is still part of the occupied Palestinian territory.[291] That is because, since the disengagement, Israel has maintained remote control over Gaza's airspace, seas, population registry, and all but one land border, thereby transforming Gaza into a "open-air prison"[292] under its control.[293]

Both technology and military dominance has allowed Israel to maintain its de facto effective control of Gaza even without a constant presence on the ground. Under the concepts of occupation presented in IHL, effective control is more important than permanent presence of troops on the ground. Thus, the predominant international position is that Israel continues to be an occupying power in Gaza and is governed by belligerent occupation law, including GCIV in terms of civilian protection.[294]

In addition, it is important to highlight that following October 7, 2023, the Israeli military resumed a regular presence on the ground in several areas within the Gaza Strip as a part of large-scale operations. Therefore, this physical presence on the ground only reinforces the

---

[286] See more at: United Nations. (2005). *The Israeli 'Disengagement' Plan: Gaza Still Occupied*. United Nations Information System on the Question of Palestine (UNISPAL). Retrieved from: https://www.un.org/unispal/document/auto-insert-205755/

[287] See more at: International Committee of the Red Cross. (2024, July 26). *What does the law say about the responsibilities of the Occupying Power in the occupied Palestinian territory?* Retrieved from: https://www.icrc.org/en/document/ihl-occupying-power-responsibilities-occupied-palestinian-territories

[288] See more at: United Nations General Assembly. (2023, September 5). *Report of the Independent International Commission of Inquiry on the Occupied Palestinian Territory, including East Jerusalem, and Israel* (A/78/198). Retrieved from: https://www.un.org/unispal/document/report-coi-palestine-isreal-a78-198/ and United Nations General Assembly. (2021, December 10). *Assistance to the Palestinian people* (A/RES/76/126). Retrieved from: https://www.un.org/unispal/document/assistance-to-the-palestinian-people-ga-resolution-a-res-76-126-2/

[289] See more at: International Criminal Court, Pre-Trial Chamber I. (2021, February 5). *Decision on the 'Prosecution request pursuant to article 19(3) for a ruling on the Court's territorial jurisdiction in Palestine* (ICC-01/18-143). Retrieved from: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2021_01165.PDF

[290] See more at: Amnesty International. (2017, June 5). *Israel's occupation: 50 years of dispossession*. Retrieved from: https://www.amnesty.org/en/latest/campaigns/2017/06/israel-occupation-50-years-of-dispossession/ and Human Rights Watch. (2021, April 27). *A threshold crossed: Israeli authorities and the crimes of apartheid and persecution*. Retrieved from: https://www.hrw.org/report/2021/04/27/threshold-crossed/israeli-authorities-and-crimes-apartheid-and-persecution

[291] Kmiotek, C. (2024, October 29). *Israel claims it is no longer occupying the Gaza Strip. What does international law say?* Atlantic Council. Retrieved from: https://www.atlanticcouncil.org/blogs/menasource/gaza-israel-occupied-international-law/

[292] See more at: Human Rights Watch. (2022, June 14). *Gaza: Israel's 'Open-Air Prison' at 15*. Retrieved from: https://www.hrw.org/news/2022/06/14/gaza-israels-open-air-prison-15

[293] Human Rights Watch. (2023, October 27). *How does international humanitarian law apply in Israel and Gaza?* Retrieved from: https://www.hrw.org/news/2023/10/27/how-does-international-humanitarian-law-apply-israel-and-gaza

[294] See supra note 291.

dominant stance that Gaza is still under occupation, currently not only through effective remote control but also by direct military presence. [295]

It is important to note that there have been some legal debates of the assessment of the nature of the armed conflict in Gaza. On one hand there are some scholars who argue that the conflict in Gaza constitutes a Non-International Armed Conflict (NIAC). The basis of this argument is that the involvement of actors like Hamas that is not a recognized state, means the conflict falls under the view of NIACs. This means that the conflict is governed by Common Article 3 of the Geneva Conventions and Additional Protocol II.[296] On the other hand, several legal scholars support classifying the conflict as an International Armed Conflict (IAC). This viewpoint is based on the claim that even though Israel is not a party to the Geneva Conventions' Additional Protocol I (AP I), some of its requirements are recognized as customary international law. This means they apply to all states, regardless of ratification. With special attention on Article 1(4) of AP I that broadens the definition of IACs to include armed conflicts in which peoples fight against colonial dominance, alien occupation, or racist regimes in the exercise of their right to self-determination, which is a provision relevant to the Palestinian situation.[297]

Therefore, legal experts have debated how to classify the armed conflict in Gaza. However, recent developments further indicate that Israel's confrontations with Palestinian armed organizations in Gaza constitute an IAC, especially during the current events post October 7th.

The International Criminal Court (ICC) considered the basis of the classification of the armed conflict in Gaza before issuing arrest warrants for senior Israeli officials[298]. The Court recognized Israel's activities in Gaza to be part of a larger context of military occupation, and the relevant legal crimes committed by Israel inside Gaza fall within the scope of an IAC.[299]

---

[295] See more at: Middle East Eye. (2024, November 13). *Israeli army 'preparing for years-long presence in Gaza'*. Middle East Eye. Retrieved from: https://www.middleeasteye.net/news/israeli-army-preparing-years-long-presence-gaza

[296] See more at: Schmitt, M. N. (2024, August 13). *Total defeat of Hamas: The end of a NIAC?* Lieber Institute West Point. Retrieved from: https://lieber.westpoint.edu/total-defeat-hamas-end-niac/

[297] See more at: Coop, S. (2024). *The Israel-Palestine conflict from the perspective of international humanitarian law* (Expert Comment No. 2024-11). Japanese Society of International Law. Retrieved from: https://jsil.jp/wp-content/uploads/2024/07/expert2024-11.pdf

[298] See more at: International Criminal Court. (2024, November 21). *Situation in the State of Palestine: ICC Pre-Trial Chamber I rejects the State of Israel's challenges to jurisdiction and issues warrants of arrest for Benjamin Netanyahu and Yoav Gallant*. Retrieved from: https://www.icc-cpi.int/news/situation-state-palestine-icc-pre-trial-chamber-i-rejects-state-israels-challenges

[299] Haque, A. A. (2024, December 12). *The International Criminal Court's classification of armed conflicts in the situation in Palestine*. Just Security. Retrieved from: https://www.justsecurity.org/105677/icc-classification-armed-conflicts-palestine/

This position was also supported by the previous Israeli Supreme Court's 2006 judgment, which had noted that Israel's confrontation with Palestinian armed organizations constituted an international armed conflict. The Court even referred to a scholar named Antonio Cassese's opinion to affirm that an "armed conflict which takes place between an Occupying Power and rebel or insurgent groups—whether or not they are terrorist in character—in an occupied territory, amounts to an international armed conflict."[300]

As a result, when Israeli military operations target Gaza, which is a territory that is recognized as part of the occupied Palestinian territory, and are directed against Palestinians, then the hostilities should be treated as part of an IAC under international law, because it falls within the general confrontations between Israel as the occupying power and the State of Palestine as the occupied.

Therefore, given the fact that there is an international consensus that Gaza remains occupied, the legal framework governing the context is that of an IAC. Under IHL occupation, it is always considered a form of international armed conflict. As validated by the ICRC legal experts who highlighted that "For the purposes of IHL, occupation is a type of international armed conflict. The laws of occupation are contained primarily in the Hague Regulations of 1907, the Fourth Geneva Convention of 1949 and its Additional Protocol I and in customary IHL."[301]

Thus, even if the detailed specificity of the armed conflict's classification in Gaza is still questioned, it is very essential to highlight that the GCIV is fully applicable during active hostilities in the context of occupation. In such context, the rights provided to civilians by GCIV including distinction, proportionality, precautions and the prohibition of collective punishment are fully binding on Israel as the occupying power in the region.

In addition to the applicability of IHL, IHRL also continues to apply in Gaza. The ICJ has confirmed that human rights treaties continue to apply extraterritorially in occupied territory and during armed conflict. Israel is a signatory to fundamental human rights treaties such as the ICCPR, but just as it does in the West Bank, Israel has long questioned the treaties' relevance to Palestinians in Gaza, citing a lack of jurisdiction or effective control. However,

[300] See supra note 277.
[301] Orkin, M., & Ferraro, T. (2022, July 26). *IHL and occupied territory*. Humanitarian Law & Policy Blog. International Committee of the Red Cross. Retrieved from: https://blogs.icrc.org/law-and-policy/2022/07/26/armed-conflict-ukraine-ihl-occupied-territory/

the ICJ has also debunked this.[302] Similarly, the UN Human Rights Committee, which oversees the ICCPR, has emphasized the need of governments ensuring the rights of all people under their power or effective control, including those living outside their borders.[303] What this means in the context of Gaza is that Israel's activities in the region can be judged under IHRL criteria such as the right to life, privacy, and due process, as well as IHL regulations. Even though IHL is considered the *lex specialis*[304], meaning the specialized law that manages hostilities, IHRL also provides another important foundation to protect individuals.[305] Therefore, despite those active hostilities in an occupation context evoke the applications of IHL including all provisions of the GCVI, IHRL does not cease to apply.

Thus, the legal framework in Gaza, during active hostilities, operates in parallel, where IHL rules the conduct of hostilities, while IHRL imposes ongoing obligations to defend basic rights. This dual approach establishes the groundwork for evaluating cyber espionage and digital military techniques under both IHL and IHRL.

After having established the legal framework applicable in Gaza, the next section explains how the cyber espionage tools used against civilians are used as a military tool. This is essential because it highlights the need to assess these practices under the legal rules governing the conduct of hostilities, particularly the principles of distinction, proportionality, and precaution.

5.1.2 Cyber Espionage as a Military Tool in Gaza

The Israeli occupation in Gaza that is ongoing, has progressively included more modern technological methods of warfare, including cyber espionage and specifically mass surveillance, into its military operations on Gaza. After decades of what is a form of traditional kinetic warfare in Gaza, Israel's strategy now largely focuses on digital covert intelligence gathering and cyber operations as sources of force. The long-term blockade and recurring

[302] International Court of Justice. (2024, July 19). *Summary of the Advisory Opinion of 19 July 2024: Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem*. Retrieved from: https://www.icj-cij.org/node/204176

[303] Human Rights Committee. (2004, May 26). *General comment No. 31: The nature of the general legal obligation imposed on States Parties to the Covenant* (CCPR/C/21/Rev.1/Add.13), para. 10. United Nations. Retrieved from: https://www.refworld.org/legal/general/hrc/2004/en/52451

[304] "This Latin term is derived from the legal maxim in the interpretation of laws, both in domestic and international law: 'lex specialis derogat legi generali'. This essentially means that more specific rules will prevail over more general rules. The term is frequently used in describing the relationship between international humanitarian law and international human rights law." See: International Committee of the Red Cross. (n.d.). Lex specialis. ICRC Casebook.

[305] See supra note 302.

hostilities from 2005 and up until the latest resumption of active hostilities that began on October 7, 2023, and are still ongoing to this day[306], have all accorded with the rise of what some call a "digital occupation," in which Israel uses technological superiority to monitor and control the population from afar.[307]

In addition, there is also another impact, which is the requirement to conduct legal reviews of new weapons or methods, as articulated by Article 36 of AP I. Although Israel is not a signatory to AP I, the notion of weapons review is widely recognized.[308] Arguably, an AI-driven targeting system like "Lavender", "The Gospel" and "Where's Daddy?" should be thoroughly reviewed to ensure that it does not violate IHL, such as by effectively targeting civilians. Some legal experts are urging the treatment of cyber/AI systems as weapon systems that must be inspected. Furthermore, international criminal law may come into play, because if cyber espionage enabled targeting results in major violations, for example, knowingly directing attacks against civilians or mass destruction, commanders may face individual criminal charges for war crimes.[309]

On a final note, there have been increasing charges recently that these Israeli cyber espionage activities enable crimes. During the active hostilities that are actively taking place in Gaza post October 7th, 2023, some Palestinian organizations and even some international observers have highlighted that Israel's campaign could be a form of digital-driven genocide, because of its systematic targeting of Palestinians, including civilians, through these big-data surveillance

---

[306] See the timeline of the active hostilities in Gaza at :Al Jazeera. (2022, August 7). *Timeline: Israel's attacks on Gaza since 2005*. Retrieved from: https://www.aljazeera.com/news/2022/8/7/timeline-israels-attacks-on-gaza-since-2005 and then, Anera. (2024, May 6). *7 months of war on Gaza: A timeline of events and humanitarian response*. Retrieved from: https://www.anera.org/gaza-war-timeline/

[307] See more at: Helga Tawil-Souri. (2012). Digital Occupation: Gaza's High-Tech Enclosure. Journal of Palestine Studies, 41(2), 27–43. https://doi.org/10.1525/jps.2012.xli.2.27

[308] See more at: International Committee of the Red Cross. (2006). *A guide to the legal review of new weapons, means and methods of warfare: Measures to implement Article 36 of Additional Protocol I of 1977*. Geneva: ICRC. Retrieved from: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0902.pdf

[309] See more at: Deeks, A. (2024, October 21). *Using artificial intelligence in warfare creates constitutional concerns, argues professor*. University of Virginia School of Law. Retrieved from: https://www.law.virginia.edu/news/202410/using-artificial-intelligence-warfare-creates-constitutional-concerns-argues-professor#:~:text=Professor%20Ashley%20Deeks%20of%20the%20University%20of%20Virginia,new%20paper%2C%20%E2%80%9C%20Delegating%20War%20Initiation%20to%20Machines.%E2%80%9D , and Human Rights Watch. (2025, April 28). *A hazard to human rights: Autonomous weapons systems and digital decision-making*. Retrieved from: https://www.hrw.org/report/2025/04/28/hazard-human-rights/autonomous-weapons-systems-and-digital-decision-making

and AI tools, that may indicate an intent to destroy a group, in whole or in part.[310] In a report in December 2024, for example, Amnesty International concluded that Israeli troops were committing "acts of genocide" in Gaza, talking about the indiscriminate bombardment and massive civilian casualties.[311] Thus, the connection between the extensive surveillance as cyber espionage tools and lethal force that may make the killing more widespread, raises the stakes for legal accountability. Therefore, the Israeli cyber espionage methods that are being used in Gaza are not a value-neutral intelligence operation. Instead, they are tools of warfare that have a direct role in tracking human targets and guiding military attacks.

Thus, after having discussed the legal framework in Gaza, where both IHL and IHRL apply with IHL being the specialized law governing the active hostilities, and after having discussed how the cyber espionage tools in Gaza specifically during the ongoing hostilities following October 7, 2023, are being used as military tools, the next section assesses their compliance of with core principles IHL. The analysis places particular emphasis on IHL as the primary framework regulating conduct during armed conflict.

5.2 The Principle of Distinction: Cyber Espionage Generated Targets

This section looks deeply at the legality of Israeli cyber espionage enabled targeting techniques in Gaza through the lens of the IHL concept of distinction, which states that parties to a conflict must always distinguish between civilians and combatants. The employment of modern surveillance technology, predictive profiling, as tools of cyber espionage, and algorithm-based target selection raises questions regarding the legality of determining legitimate military targets.

[310] See more at: Rahman, A. (2024, October 16). *Explainer: The role of AI in Israel's genocidal campaign against Palestinians*. Institute for Palestine Studies. Retrieved from: https://www.palestine-studies.org/en/node/1656285, Katibah, L. (2024, October). *The genocide will be automated—Israel, AI and the future of war*. Middle East Report, (312). Middle East Research and Information Project. Retrieved from: https://merip.org/2024/10/the-genocide-will-be-automated-israel-ai-and-the-future-of-war/, and Pietralunga, C. (2024, April 5). *Israeli army uses AI to identify tens of thousands of targets in Gaza*. Le Monde. Retrieved from: https://www.lemonde.fr/en/international/article/2024/04/05/israeli-army-uses-ai-to-identify-tens-of-thousands-of-targets-in-gaza_6667454_4.html

[311] Amnesty International. (2024, December 5). *Amnesty International concludes Israel is committing genocide against Palestinians in Gaza*. Retrieved from: https://www.amnesty.org/en/latest/news/2024/12/amnesty-international-concludes-israel-is-committing-genocide-against-palestinians-in-gaza/

5.2.1 Civilian vs. Combatant

According to one of IHL's foundation principles which is distinction, parties to a conflict must always distinguish between combatants and civilians and direct their attacks only against the former. This means that civilians may never be attacked unless they directly participate in hostilities. This has been articulated in Article 27 of GCIV[312] and in Article 51(2) of AP I[313]. In addition, the ICRC has noted in customary IHL Rule 1 that the "parties to the conflict must always distinguish between civilians and combatants. Attacks may only be directed against combatants and must not be directed against civilians."[314] This rule is binding in both international and non-international armed conflicts and represents a universal norm. In the context of Gaza, this principle indicates that Israeli troops must carefully distinguish between members of armed groups, or persons participating in hostilities, and the broader civilian population. Any attack on the civilian population violates the distinction principle and is considered a grave breach, and a war crime under Article 8(2)(b)(i) of the Rome Statute[315].

In addition, as a clear definition of a civilian was not provided in the GCIV, Article 50 of AP I defines a civilian as anybody who is not a combatant. In addition, it highlights that if there is any uncertainty about whether a person is a civilian, that person is presumed to be one.[316] This implication that civilian status is given when in doubt reflects the protective objective of IHL. Although Israel is not a signatory to AP I, this article is widely accepted as customary law as it is the only available definition of a civilian.[317] In Gaza, however, the practice has frequently been the opposite, where extensive surveillance and "big data" profiling have resulted in many persons being labeled as combatants by default, even without actual evidence provided. Israeli officials regularly refer to young Palestinian boys as "militants" unless proven otherwise,

[312] See supra note 180.
[313] International Committee of the Red Cross. (1977). *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977*. Retrieved from: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977
[314] International Committee of the Red Cross. (n.d.). Rule 1. The Principle of Distinction between Civilians and Combatants. Customary IHL Database. Retrieved from: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule1
[315] International Criminal Court. (2011). *Rome Statute of the International Criminal Court*. Retrieved from: https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf
[316] See supra note 313.
[317] See more at: International Residual Mechanism for Criminal Tribunals. (2004.). *Civilian population*. ICTR/ICTY/IRMCT Case Law Database. Retrieved from: https://cld.irmct.org/notions/show/141/civilian-population

effectively shifting the weight of distinction.[318] This approach is contradictory with the IHL rule that doubts must be resolved in favor of civilian status.

The major recognized issue with cyber espionage is that it could confuse the distinction between civilians and combatants. Traditional signs of combatant identity, which are related to uniforms, publicly carrying weaponry, and connection with armed forces, are frequently absent or unreliable in asymmetric hostilities like the ones in Gaza. Therefore, Israeli intelligence uses digital factors to determine who is a combatant. Predictive analytics may identify a person as a combatant because they called a known militant, visited specific sites, and so on. However, many of the flagged people may be ordinary civilians. The principle of distinction involves an individual decision of whether a person is directly participating in hostilities or performs a continuous fighting function for an organized armed group.[319]Relying on broad profiles or algorithms increases the possibility of misclassifying civilians as combatants, which violates Article 50's criterion.[320]

Evidence from the recent hostilities in Gaza, show that Israeli forces have blurred the line between civilian and combatant, in part due to digital profiling. In late 2023, the Israeli military apparently classified tens of thousands of Gazans as prospective targets using analysis of algorithms.[321] This kind of extensive classification of people as combatants or even as “terrorists" based on big data analytics can be seen as a serious violation of both the word and spirit of the concept of distinction that is articulated in IHL. That is because it treats the entire civilian population as suspicious, inherently violates the customary principle of distinction, and also in violation of Article 51(2) of AP I, that is interlinked with the customary rule, as it states that "the civilian population as such, as well as individual civilians, shall not be the object of attack."[322]

---

[318] Abraham, Y. (2024, April 3). ‘Lavender’: The AI machine directing Israel’s bombing spree in Gaza. *+972 Magazine*. Retrieved from: https://www.972mag.com/lavender-ai-israeli-army-gaza/

[319] *Ibid.*

[320] See more at: Zhou, W., & Greipl, A. R. (2024, August 29). *Artificial intelligence in military decision-making: Supporting humans, not replacing them*. ICRC Humanitarian Law & Policy Blog. Retrieved from: https://blogs.icrc.org/law-and-policy/2024/08/29/artificial-intelligence-in-military-decision-making-supporting-humans-not-replacing-them/ICRC Blogs+2 and Viveros Álvarez, J. S. (2024, September 4). *The risks and inefficacies of AI systems in military targeting support*. ICRC Humanitarian Law & Policy Blog. Retrieved from: https://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/

[321] See supra note 144.

[322] See supra note 313.

The extent of the harm that is caused by these Israeli practices and tools raise very serious legal implications. When looking at the death toll in Gaza in the recent hostilities that has exceeded 50,000 Palestinians killed, over 100,000 injured, and thousands still missing and assumed dead, two scenarios in this context must be addressed. The first scenario is that these deaths and injuries amongst Palestinians in the Gaza Strip indicate that there are mistakes in a systematic manner within the AI tools used themselves. That could be because of automation bias, issues in the input data given, or that there is insufficient human supervision over the target. In this case, the Israeli military's reliance on this kind of predictive analytics would have resulted in an illegal and indiscriminate misidentification, which highlights the need for an individualized determination that a person is directly participating in hostilities. The second scenario is that in addition to the possibility of misidentification, civilians are targeted intentionally or in a reckless manner by Israel, which shows a policy that completely ignores the rules of distinction. It is important to highlight that in either way, the result is a pattern of attacks that disproportionately target civilians and demonstrate a lack in IHL compliance.

These two scenarios are not mutually exclusive. Because instead, they may be mutually reinforcing, as AI profiling as a form of cyber espionage, it is being used as a tool to cover illegal purposes or to speed up the mass targeting of individuals without sufficient validation. As the ICRC has highlighted, algorithms must not substitute human judgment in decisions concerning the use of fatal force. The increasing use of digital surveillance and prediction technology in armed conflict necessitates close investigation to guarantee that the principle of distinction remains fundamental in practice, rather than just in law.[323]

Thus, after having discussed in theory the need for distinction between civilians and combatants in IHL, the next section looks at the Israeli use of these cyber espionage tools, to assess if they comply with the distinction principle.

[323] See more at: International Committee of the Red Cross. (2021). *Artificial intelligence and machine learning in armed conflict: A human-centred approach*. *International Review of the Red Cross*, 102(913), 463–479. https://doi.org/10.1017/S1816383120000454 and Zhou, W., & Greipl, A. R. (2024, August 29). *Artificial intelligence in military decision-making: Supporting humans, not replacing them*. ICRC Humanitarian Law & Policy Blog. rETRIEVED FROM: https://blogs.icrc.org/law-and-policy/2024/08/29/artificial-intelligence-in-military-decision-making-supporting-humans-not-replacing-them/

5.2.2 Use of Predictive Surveillance and Profiling: Types of Cyber Espionage

In Gaza, especially most recently, the modern military cyber espionage methods use predictive profiling tools that analyze large amounts of data to identify individuals who Israel suspects to have some association with Palestinian armed groups. A valid example of this is the Israeli "Project Lavender" discussed earlier (see section 3.3.1)[324]

The use of predictive surveillance as tools of cyber espionage that were explained in detail in Chapter 2, to conduct targeted creates serious legal contemplations. First, these tools presume guilt by algorithm rather than actual evidence of participation in hostilities. This is especially true due to the suspicion score of Lavandar.[325] This has a true impact on the IHL presumption of civilian status, because it assumes many people to be combatants based on ambiguous criteria. This completely undermines the IHL presumption of civilian status since persons can be labeled as combatants based on opaque and confusing criteria that are neither revealed or available to judicial review. Therefore, since the criteria are unknown and appear to be based on indirect associations, such as digital communication patterns, social network proximity, or behavioral traits, the process fails to determine whether individuals are directly participating in hostilities as required by IHL. As a result, Israeli soldiers risk targeting people who are still protected by the law, which violates the principle of distinction.[326]

"Project Lavender" for instance shows how these cyber espionage-based profiling can identify civilians. During the early stages of the current hostilities in Gaza, the system reportedly identified 37,000 people as potential targets due to their alleged Hamas affiliations. According to US sources before October 7th, Hamas' entire military wing membership is estimated to be between 25,000 and 30,000, this statistic indicates that the net was stretched far too wide, encompassing many ordinary citizens. According to intelligence sources, Lavender's output included low-level persons with merely peripheral links to Hamas, such as civil defense officials and police officers, causing military leaders to authorize operations that included the killing of civilians to eliminate these suspicions. First, even such officers, if they do not

[324] Abraham, Y. (2024, April 3). *'Lavender': The AI machine directing Israel's bombing spree in Gaza*. +972 Magazine. Retrieved from: https://www.972mag.com/lavender-ai-israeli-army-gaza/
[325] Abreu, M., Delpuech, A., Layan, E., Batrawi, W., Rueckert, P., Jurado, S. Á., Youssef, Y., Osman, H., Abraham, Y., Carpentier, A., & Zerrouky, M. (2024, July 25). *Death from above: How Israeli drones are killing journalists in Gaza*. Arab Reporters for Investigative Journalism (ARIJ). Retrieved from: https://arij.net/investigations/gaza-project/en/israeli-drones/index.html
[326] *Ibid*.

participate directly in hostilities, are considered civilians. In addition, to kill those officers, Israel is willing to kill many civilians to get to those even though they consider them low-ranked targets. Based on testimony from two Israeli intelligence officers, during the first weeks of the war, they were allowed to kill 15 or 20 civilians during airstrikes on low-level targets. According to the reports, unguided bombs known as "dumb bombs" were often used in such attacks, destroying entire homes and killing all their occupants. One of the intelligence officers said, “you don’t want to waste expensive bombs on unimportant people – it’s very expensive for the country and there’s a shortage [of those bombs].” The other one continued saying “Because we usually carried out the attacks with dumb bombs, and that meant literally dropping the whole house on its occupants. But even if an attack is averted, you don’t care – you immediately move on to the next target. Because of the system, the targets never end. You have another 36,000 waiting.”[327]

Multiple testimonies from Israeli intelligence officers provide insight into how the Lavender system’s use went beyond mere algorithmic misclassification and into what many have described as a policy of indiscriminate targeting. One officer confessed, “We were not interested in killing [Hamas] operatives only when they were in a military building or engaged in a military activity… It’s much easier to bomb a family’s home. The system is built to look for them in these situations.” This illustrates that Lavender’s function was operationalized in a way that prioritized convenience over compliance with the principle of distinction. Another intelligence source acknowledged the resulting civilian toll: “We’ve killed people with collateral damage in the high double digits, if not low triple digits… These are things that haven’t happened before.” Some testimonies confirm that proportionality was not meaningfully considered. One officer explicitly admitted, “In practice, the proportionality criterion did not exist,” while another described the overall targeting approach as “a policy so permissive that in my opinion it had an element of revenge.” Moreover, reliance on Lavender led to extreme automation bias, with officers spending as little as 20 seconds approving each target: “I had zero added value as a human, apart from being a stamp of approval,” one said. The pressure to increase the number of targets further eroded human oversight: “We were constantly being pressured: ‘Bring us more targets.’… We were told now we have to [mess up] Hamas, no matter what the cost.” This industrial-scale approval of targets, based on opaque algorithmic

[327] See supra note 324.

suspicion scores, not only degrades the distinction principle—it facilitates mass targeting untethered from legal safeguards. [328]

Furthermore, examples from the ground are the targeting of journalists in the Gaza Strip. Journalists, as civilians who are not actively involved in hostilities, are entitled to protection. Journalists are known to be civilians unless they directly participate in hostilities, and this was reaffirmed and articulated in Article 79 of AP I.[329] In addition it is a part of customary international law, as IHL Customary Rule 34 states that "Civilian journalists engaged in professional missions in areas of armed conflict must be respected and protected as long as they are not taking a direct part in hostilities."[330] However, since the start of the active hostilities on October 7, 2023, Gaza has become a very dangerous place for journalists. According to resources, at least 226 journalists have been killed since October 7th.[331]

The nature and circumstances of these killings suggest that they were not accidental or unintentional, but rather the result of systematic and planned targeting that has often been assisted by cyber espionage enabled surveillance technologies. An in-depth investigation provides evidence that Israeli forces have repeatedly used aerial surveillance and precision drone strikes to kill journalists who were clearly identified as journalists and operating outside of combat zones. Many of these strikes came during periods of visible reconnaissance and involved the use of drone technology capable of visually confirming the press sign they were wearing, implying deliberate decisions to strike despite apparent civilian status.[332]

Among the documented cases is the killing of four journalists in Tal al-Zaatar on January 22, 2024. The victims were on the ground shooting sights of famine in Gaza and the ruins when a drone appeared over them and fired a missile. There are different types of evidence that is available like videos and other forensic evidence that show that the journalists were wearing

---

[328] *Ibid*.
[329] See supra note 313.
[330] International Committee of the Red Cross. (n.d.). *Rule 34. Denial of quarter and other forms of perfidy*. In *Customary IHL Database*. Retrieved from: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule34
[331] Newsroom. (2025, June 6). *226 journalists killed in Gaza by Israeli army since Oct. 7: Gaza Media Office*. Türkiye Today. Retrieved from: https://www.turkiyetoday.com/region/israeli-army-kills-226-journalists-in-gaza-since-october-7-3202491
[332] Abreu, M., Delpuech, A., & Layan, E. (2024, June 25). *Death from Above: How Israeli Drones are Killing Journalists in Gaza*. Arab Reporters for Investigative Journalism. Retrieved from: https://arij.net/investigations/gaza-project/en/israeli-drones/index.html

both press vests and helmets at the time of the attack. In addition, they show that there were no active hostilities taking place nearby at that time.[333]

Similarly, on December 15, 2023, Samer Abu Daqqa, Al Jazeera cameraman, was killed in Khan Younis by an Israeli drone strike while he was reporting the aftereffects of a previous Israeli attack on a UN-run school. At the time of the attack, Abu Daqqa was easily recognized as a journalist, as he was wearing visible press gear, and he clearly was working along with other journalists and emergency personnel. He was with Wael Al-Dahdouh, Al Jazeera's Gaza bureau chief, who was severely injured in the same incident. Al-Dahdouh is a very well-known figure for his constant reporting on the humanitarian impact of Israel's attacks in Gaza.[334]

After the attack on the journalists, the ambulances and civil defense rescuers were prevented from reaching Abu Daqqa for more than five hours, during which he bled to death. According to reports, at least three civil defense personnel were killed while attempting to reach the site, and medical staff were purposefully targeted or shot upon, obstructing the safe evacuation of the wounded.[335] The circumstances of this attack, including the targeting of identifiable journalists outside active combat zones and the systematic impediment to emergency response, violate the principle of distinction and protection of medical and press personnel under international humanitarian law.

It is important to note that prior to the December 15, 2023, drone attack that injured Wael Al-Dahdouh, Israeli forces had already conducted other forms of attacks on him. On October 25, 2023, while he was broadcasting live from the field, an Israeli aircraft hit the house where his immediate family were seeking refuge after being displaced. The attack killed several members of his family, including his wife, 2 of his children, and one of his grandchildren, as well as more than 20 other civilians, many of them directly related to Al-Dahdouh. Even though Israel did not openly admit that the attack was intentional, some experts saw its timing, context, and consequence as a calculated act of psychological warfare designed to intimidate the press and

---

[333] *Ibid.*

[334] See more at: Abreu, M. (2025, March 27). *"Where international law goes to die": Mechanisms blocking justice for journalists and civil society* [Gaza Project]. Forbidden Stories. Retrieved from: https://forbiddenstories.org/palestine-international-law-journalists-society/, Committee to Protect Journalists. (2023, December 15). *Samer Abu Daqqa*. CPJ. Retrieved from: https://cpj.org/data/people/samer-abu-daqqa/

[335] Al Jazeera Media Network. (2023, December 15). *Al Jazeera condemns Israeli forces killing of cameraman Samer Abudaqa*. Al Jazeera. https://www.aljazeera.com/news/2023/12/15/al-jazeera-condemns-israeli-forces-killing-of-cameraman-samer-abu-daqqa

RFI. (2023, December 16). *Funeral held for Al Jazeera journalist killed in Israel strike*. RFI. Retrieved from: https://www.rfi.fr/en/middle-east/20231216-funeral-held-for-al-jazeera-journalist-killed-in-israel-strike

journalists. This tactic was done hand in hand with Israeli authorities' repeated attempts to completely shut down Al Jazeera's operations by canceling its license and blocking its transmissions, within the occupied territory.[336]

In this context, cyber espionage can also be seen as a key enabler of targeted repression. The accumulated evidence available includes eyewitness testimonies, drone footage, and expert analysis, which all support the notion that journalists in Gaza are targeted based on digital associations and algorithmic profiling, rather than conduct. Many of the journalists killed had been digitally surveilled, with AI systems like Lavender potentially flagging their metadata and communications and visually verifying their identities before they were killed. This technical architecture, which combines cyber espionage, AI, and drone warfare, has created a situation in which the customary protections that are provided to civilians under IHL are ignored.[337] This thus violates the customary rule of distinction, in addition to the customary rule of protecting journalists.

Therefore, when these examples are closely studied, it can be argued that the use of cyber espionage tools in Gaza is also associated with collective punishment techniques that are prohibited under Article 33 of GVIC[338] and Customary IHL Rule 103[339]. For instance, this is highlighted by documents and media reports on the Israel's algorithmic tool "The Gospel." A former Israeli intelligence officer clearly stated that these tools are being used to "lead civilians to put pressure on Hamas." This includes attacking huge residential buildings or utilities, not for immediate military benefit, but to psychologically damage the civilian population and indirectly diminish Hamas support. Therefore, such tools used by Israel, by definition, cause civilian harm that is not proportionate to concrete military advantage, especially if the declared

---

[336] See more at: Malik, N. (2024, October 31). *'I couldn't cry over my children like everyone else': The tragedy of Palestinian journalist Wael al-Dahdouh*. The Guardian. Retrieved from: https://www.theguardian.com/world/2024/oct/31/wael-al-dahdouh-gaza-palestinian-journalist-tragedy, Al Jazeera Media Network. (2023, October 25). *Al Jazeera condemns killing of journalist Wael Al-Dahdouh's family in Gaza*. Al Jazeera. Retrieved from: Westfall, S., & Berger, M. (2023, October 26). *Family of Al Jazeera Gaza bureau chief killed in airstrike*. The Washington Post. https://www.washingtonpost.com/world/2023/10/25/wael-al-dahdouh-family-gaza-al-jazeera/https://www.aljazeera.com/news/2023/10/25/al-jazeera-condemns-killing-of-journalist-wael-al-dahdouhs-family-in-gaza
Westfall, S., & Berger, M. (2023, October 26). *Family of Al Jazeera Gaza bureau chief killed in airstrike*. The Washington Post. Retrieved from: https://www.washingtonpost.com/world/2023/10/25/wael-al-dahdouh-family-gaza-al-jazeera/

[337] See supra note 332.

[338] See supra note 180.

[339] International Committee of the Red Cross. (n.d.). Rule 103. Collective Punishments. In Customary International Humanitarian Law, Volume I: Rules. Retrieved from: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule103:contentReference[oaicite:6]{index=6}

purpose is civilian coercion.[340] The concept of these attacks being linked to collective punishment was also verified in a report by the UN Human Rights Office, as it was noted that "under certain circumstances, the deliberate destruction of healthcare facilities may amount to a form of collective punishment, which would also constitute a war crime." In addition, they added "if committed as part of a widespread or systematic attack directed against a civilian population, further to a State or, in case of non-State actors, organizational policy, may also amount to crimes against humanity."[341]

Therefore, the intent is clearly to inflict fear amongst people to put pressure on armed groups, this also directly implicates Customary IHL Rule 2, which prohibits "acts or threats of violence the primary purpose of which is to spread terror among the civilian population."[342]

In addition, a particular example of the type of terror that is inflicted on the civilians in Gaza is the continued use of surveillance drones as a tool for cyber espionage, in Gaza's skies. The name "Zanana," used by Palestinians to describe the incessant drone of surveillance UAVs, as the ones used in the West Bank, represent the persistent sense of being watched, followed, and in Gaza specifically, potentially targeted at any time. According to reports, this continual aerial presence has caused considerable psychological harm to civilians. One mother stated that "the moment my child hears the sound of the drone, he runs and sits in my lap… I find no words to calm him."[343] Though drone monitoring is not specifically or directly illegal, its continued use in a way that aims to install fear without a proven military purpose may cross the line from precautionary surveillance to psychological warfare. As one resident put it, "we live in a military camp. The drone transforms Gaza into a field of war."[344] Reports also described the drones as a "mechanism of control and fear, amplifying a vertical politics of power" where Israel acts as "watcher, judge, jury and executioner" over Palestinians below.[345]

---

[340] See supra note 165.
[341] Office of the United Nations High Commissioner for Human Rights. (2024, December 31). *Thematic report – Attacks on hospitals during the escalation of hostilities in Gaza (7 October 2023–30 June 2024)*. United Nations. Retrieved from: https://www.ohchr.org/sites/default/files/documents/countries/opt/20241231-attacks-hospitals-gaza-en.pdf
[342] International Committee of the Red Cross. (n.d.). *Rule 2. Violence aimed at spreading terror among the civilian population*. Customary International Humanitarian Law. Retrieved from: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule2
[343] Skinner, C. (2019). *'Precise' strikes: Fractured bodies, fractured lives – Israel's drone wars: An update* (p. 18). Drone Wars UK. Retrieved from: https://dronewars.net/wp-content/uploads/2019/11/DW-FracturedLives-WEB.pdf
[344] *Ibid.*
[345] *Ibid.*

Thus, the psychological impact is more than just a side effect, as it has legal implications when it is caused by techniques that disrespect the principle of differentiation, considering all civilians as suspects who need to be constantly monitored, and fearful.

In conclusion, the use of predictive surveillance tools as cyber espionage methods like Project Lavender in Gaza blatantly wears down the distinction between civilian and combatant. That is because it relies on big data profiling and algorithmic suspicion scores. Therefore, Israeli forces have effectively turned civilians into targets based on speculative criteria, constituting a considerable deviation from IHL's protections. Furthermore, when such tools are employed systematically to subject the entire community to persistent fear, suspicion, and violence, they contribute to a larger pattern of collective punishment.

Thus, after concluding that Israel's use of cyber espionage as a military tool in Gaza fails to comply with the principle of distinction, the next section examines the underlying causes of this failure, specifically whether they stem from automation bias and technological malfunctions or reflect a deliberate Israeli policy. This is essential because establishing intent or systemic negligence is critical for determining legal responsibility and future accountability under international law.

5.2.3 Automation Bias or an Israeli Policy? Structural Failures in Distinction

Israel's use of AI-powered cyber espionage tools that lead to targeting such as Project Lavender has created severe legal concerns, especially with the problem of automation bias, which is the tendency for operators to place undue reliance on machine-generated results. As a report by Human Rights Watch shows, Lavender and other AI cyber espionage tools Israel uses have more than one structural weakness. For instance, there is the "black box" nature of its decision-making. That means that machine learning, AI, and other algorithmic systems in general, by their definition, do not allow for inspection or clear transparency into their work or decision-making processes. Thus, they lack the documentation needed to enable assigning accountability to certain key players. It is very critical for digital tools to allow users to inspect the systems' outputs, see how they were generated, and which data was used. This is very crucial when it comes to AI-powered weapons or target generating systems. In addition, algorithms trained on discriminatory or overly broad criteria are likely to reproduce and amplify existing prejudices, for example, the notion that all adult males in Gaza are potential militants, thus compromising

the essential IHL obligation to separate civilians from combatants. In fact, this process which is referred to as "garbage in, garbage out" dynamic can result in major misclassifications. [346]

However, what is very important is that these technological risks do not occur in isolation, especially as mentioned, the issue is with the information being fed to the AI tools. Therefore, this must be understood in the context of Israel's military and political policies regarding Gaza. To be more precise, following the commencement of the recent active hostilities in Gaza following October 7, 2023, key Israeli authorities made public statements that show a clear readiness to dilute or perhaps remove the civilian-combatant line. For instance, Israeli President Isaac Herzog declared that "an entire nation" was responsible for Hamas's actions, rejecting the idea that Palestinian civilians in Gaza were uninvolved.[347] On a similar note, Israeli Defense Minister Yoav Gallant noted that he had "ordered a complete siege on the Gaza Strip. There will be no electricity, no food, no fuel, everything is closed. We are fighting human animals, and we are acting accordingly."[348] Defense Minister Avigdor Lieberman claimed that "there are no innocent people in Gaza. Everyone's connected to Hamas, everyone gets a salary from Hamas. "[349] Furthermore, Moshe Feiglin, a former member of the Knesset, publicly stated that "every child, every baby in Gaza is an enemy. The enemy is not Hamas, nor is it the military wing of Hamas. We need to conquer Gaza and colonize it and not leave a single Gazan child there. There is no other victory."[350] In addition, and perhaps most notably, Israeli Prime Minister Benjamin Netanyahu cited a biblical verse that calls for the complete destruction of an enemy population, including "man and woman, infant and suckling."[351] Therefore, all these statements cannot be seen as merely isolated incidents, because they very clearly reflect a

[346] See supra note 165.
[347] McGreal, C. (2023, October 16). *The language being used to describe Palestinians is genocidal*. The Guardian. Retrieved from: https://www.theguardian.com/commentisfree/2023/oct/16/the-language-being-used-to-describe-palestinians-is-genocidal
[348] Fabian, E. (2023, October 9). *Defense minister announces 'complete siege' of Gaza: No power, food or fuel*. The Times of Israel. Retrieved from: https://www.timesofisrael.com/liveblog_entry/defense-minister-announces-complete-siege-of-gaza-no-power-food-or-fuel/
[349] The New Indian Express. (2018, April 8). *There are no innocent people in Gaza: Israel defence minister Avigdor Lieberman*. Retrieved from: https://www.newindianexpress.com/world/2018/Apr/08/there-are-no-innocent-people-in-gaza-israel-defence-minister-avigdor-lieberman-1798750.html
[350] NDTV News Desk. (2025, May 22). *"Every baby in Gaza is an enemy": Ex-Israeli lawmaker's shocking remarks*. NDTV. Retrieved from: https://www.ndtv.com/world-news/moshe-feiglin-every-baby-in-gaza-is-an-enemy-ex-israeli-lawmakers-shocking-remarks-8477020
[351] Middle East Monitor. (2023, October 29). *Netanyahu declares holy war against Gaza, citing the Bible*. Retrieved from: https://www.middleeastmonitor.com/20231029-netanyahu-declares-holy-war-against-gaza-citing-the-bible/

broader ideological orientation that treats the civilian population as inherently complicit and thus targetable.

What is also important to highlight is that the Israeli tendency to conflate civilians with combatants is not new or specific to the recent ongoing hostilities. That is because as early as 2009, during what the Israeli government called the "Cast Lead operation" in Gaza, Amnesty International reported that an Israeli army spokesperson told the BBC: "Our definition is that anyone who is involved with terrorism within Hamas is a valid target. This ranges from the strictly military institutions and includes the political institutions that provide the logistical funding and human resources for the terrorist arm." Amnesty International has warned in that report that in many armed conflicts, civilians are deliberately targeted under the appearance of redefining who qualifies as a military objective, stating that direct attacks on civilians "are often justified by denying that the victims are actually civilians... Civilian immunity is also undermined by the manner in which definitions of military objectives and civilian objects are interpreted by attacking forces." This term very significantly broadens the pool of targetable individuals, violating IHL's restriction that only those directly involved in hostilities be legitimately attacked.[352]

The Israeli already broad understanding has only broadened further in recent years. For example, in a 2023 interview, Israeli National Security Minister Itamar Ben-Gvir stated that "to be clear, when they say that Hamas needs to be eliminated, it also means those who sing, those who support, and those who distribute candy, all of these are terrorists. They should all be eliminated."[353]

This therefore indicates a deeply ingrained belief that almost every element of Gaza's population is linked with "terrorism". As a result, the Israeli strategy appears to completely blur the boundary between civilians and fighters, thereby portraying Gaza's whole population as a single adversary. This ideological posture allows for, and, in some cases, encourages the targeting policies that violate the key IHL concept of distinction.

[352] Amnesty International. (2009). *Israel/Gaza: Operation 'Cast Lead': 22 days of death and destruction* (MDE 15/007/2009). Retrieved from: https://www.amnesty.org/en/documents/MDE15/007/2009/en/

[353] Middle East Monitor. (2023, November 12). *Anyone who supports Hamas should be eliminated: Israeli minister*. Retrieved from: https://www.middleeastmonitor.com/20231112-anyone-who-supports-hamas-should-be-eliminated-israeli-minister/

Thus, in this context, the risks associated with AI-driven classifications as forms of cyber espionage that are directly used for targeting, are more than just technological faults, they are facilitated and reinforced by legislation. Therefore, the systemic use of tools like Lavender, which is a cyber espionage tool, without meaningful human oversight or transparency, combined with the Israeli official rhetoric that completely ignores the legal protections afforded to civilians, creates an operational environment in which violations of the principle of distinction are not just more likely but are also structurally rooted.

Under IHL, all states must make reasonable efforts to ensure that targets are legitimate combatants. Therefore, the failure to do so, especially in a context where civilians are widely seen as suspects, results in indiscriminate strikes or even war crimes. Furthermore, when digital profiling as a tool of cyber espionage is used in a context that appears to accept or excuse civilian killings, the burden of legal accountability shifts from individual error to institutional purpose.

Finally, the use of AI as a tool for cyber espionage in targeting must be evaluated not just by the algorithms' performance, but also by the policies that govern their use. Thus, when taking a close look at Gaza, the combination of opaque digital technologies, automation bias, and outright dehumanization of people shows a complete disregard for the principle of differentiation. Importantly the violation of this principle could also amount to war crimes as it could violate Article 8(2)(b)(i)[354] and Article 8(2)(b)(iv)[355] of the Rome Statute. It also could amount to crimes against humanities as they could violate Article 7(1)(a)[356] of the Rome Statute.[357]

Thus, after explaining in detail Israel's failure to meet the distinction principle, the next section examines Israel's compliance with the principles of proportionality and precaution.

[354] "Intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities;" See more at: United Nations. (1998). *Rome Statute of the International Criminal Court*.
[355] "Intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated;" See more at *Ibid*.
[356] "Murder;" See more at *Ibid*.
[357] *Ibid.*

5.3 Proportionality and Precaution in Cyber Espionage Enabled Attacks

As the previous section examined the principle of distinction, the principles of proportionality and precaution are also essential components of IHL, especially in the context of active hostilities. These principles illustrate that states, as they launch attacks, must always ensure that the predicted incidental harm to civilians is proportionate to the anticipated concrete and direct military advantage. In addition, the states must take all reasonable efforts to minimize civilian suffering and harm. Therefore, this section studies if the Israeli cyber espionage tools facilitate attacks that pose major concerns under the proportionality and precautionary principles.

5.3.1 Proportionality in Cyber Espionage Enabled Targeting

In addition to distinction, IHL also prohibits attacks that, even if directed at a legitimate military objective, cause excessive civilian harm in comparison to the expected military advantage. This is the proportionality rule for attacks. This rule is considered part of the international customary law, as it is articulated in c**ustomary IHL Rule 14**, as it states that *"Launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects… which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited."*[358] In practice, this means that commanders must assess the probable civilian casualties against the value of the target, canceling any strike where the civilian cost obviously outweighs the advantage. When taking a close look at the situation in Gaza, where military targets are frequently integrated in civilian neighborhoods, proportionality judgments are very crucial. The cyber espionage driven targeting has occasionally permitted treating a little military gain as sufficient justification for a large human toll.

In Gaza, proportionality concerns have been especially obvious in attacks that were directed at protected civilian facilities such as hospitals, religious sites, and schools. Typically, Israel justifies these attacks based on an alleged terrorist presence. For instance, following October 7, 2023, Israel targeted various medical facilities, including Al-Shifa, Al-Quds, and the Indonesian Hospitals, saying that Hamas exploited them for military activities.[359] The attack

[358] Henckaerts, J.-M., & Doswald-Beck, L. (2005). *Customary international humanitarian law: Volume I: Rules*. International Committee of the Red Cross. Retrieved from: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule14

[359] See more at: Office of the United Nations High Commissioner for Human Rights. (2024, December 31). *Pattern of Israeli attacks on Gaza hospitals raises grave concerns: Report*. Retrieved from: https://www.ohchr.org/en/press-releases/2024/12/pattern-israeli-attacks-gaza-hospitals-raises-grave-concerns-

on Al-Shifa Hospital, Gaza's largest and most important hospital complex, was apparently centered on signals intelligence and allegations that Hamas had command facilities beneath the compound and may even be keeping some of the "hostages" there.[360] Some U.S. officials also made these assertions, making reference to confidential intelligence assessments.[361] However, the material made public was limited and did not confirm the existence of Hamas militants, military infrastructure or "hostages" within the hospital. Independent investigators, including Human Rights Watch and media sources such as The Washington Post, discovered no proof that hospitals were being utilized to conceal military operations. In addition, it was determined that these attacks "should be investigated as war crimes."[362]

These attacks on Gaza hospitals have all resulted in civilian casualties, including patient deaths, the collapse of critical care infrastructure, and the complete breakdown of health services. Even though Israel claims that there were military objectives, the extent of civilian suffering greatly surpassed any expected advantage, especially since no evidence was found to support Israel's claims.[363] Thus, these strikes that are typically done with cyber espionage tools assistance, are obviously disproportionate under IHL.

In addition to bombing hospitals, Israeli bombings on Gaza schools have also caused civilian casualties, because these schools had thousands of displaced families seeking shelter. Israeli authorities also justify these attacks by claiming that Hamas uses these facilities for military purposes, again despite a lack of clear evidence.

For example, on August 10, 2024, an Israeli airstrike hit the Al-Tabaeen School in Gaza City, which was used as a shelter for displaced civilians. The attack killed at least 80 people and injured almost 50. The Israeli military claimed it targeted a Hamas command center within the school compound but provided no proof to back up this claim. Israel claimed that the

---

report and United Nations. (2025, January 3). *Security Council debates Israeli attacks on hospitals allegedly misused by Hamas, as UN rights chief urges independent probes* (Press Release No. SC/15959). Retrieved from: https://press.un.org/en/2025/sc15959.doc.htm

[360] Human Rights Watch. (2023, November 14). *Gaza: Unlawful Israeli hospital strikes worsen health crisis*. Retrieved from: https://www.hrw.org/news/2023/11/14/gaza-unlawful-israeli-hospital-strikes-worsen-health-crisis

[361] See more at: Gomez, J., Martinez, L., & Crawford, S. K. (2023, November 14). *US says it has intelligence Hamas has used Gaza's Al-Shifa Hospital to hold hostages*. ABC News. Retrieved from: https://abcnews.go.com/International/us-intelligence-hamas-gazas-al-shifa-hospital-hold/story?id=104887035 and Nakashima, E., & Loveluck, L. (2024, January 3). *U.S. 'confident' that Hamas used al-Shifa Hospital as command center*. The Washington Post. Retrieved from: https://www.washingtonpost.com/national-security/2024/01/03/hamas-gaza-israel-alshifa-tunnels/

[362] See supra note 360.

[363] *Ibid*.

precautions it took to reduce the risk to people included the use of a "small warhead," aerial observation, and intelligence information. However, the UN Human Rights Office described Israel's attacks on schools as "systematic."[364] The director of Al-Fathi hospital that received the injured noted that "We received some of the most serious injuries we encountered during the war," as many of the wounded had limbs amputated and some with severe burns. An eyewitness noted that "there were people praying, there were people washing and there were people upstairs sleeping, including children, women and old people, the missile fell on them without warning. The first missile, and the second. We recovered them as body parts."[365]

These types of strikes are not limited to public facilities, as there have also been massive attacks on civilian private structures. For instance, on October 31, 2023, an Israeli airstrike attacked a six-story residential structure in central Gaza, killing at least 106 civilians, including 54 children, in one single strike. The structure housed around 350 individuals, as many of them have been displaced earlier. According to a report by Human Rights Watch, the strike involved four aerial missiles impacting the structure within roughly 10 seconds, resulting in its total destruction. In the thorough report, evidence was gathered through interviews, examination of satellite imagery, photographs, and videos, the result was that there was no evidence of a military target within or around the facility at the time of the strike. Israeli officials provided no rationale or information regarding the alleged target. This lack of transparency, along with the high civilian casualty toll and the absence of a visible military aim, prompted the report to classify the strike as an apparent war crime.[366]

It is also essential to note that violations of proportionality in targeting operations can concurrently amount to breaches of the right to life under international human rights law, particularly Article 6 of the ICCPR. As previously argued, even in the context of an armed conflict, as established before, IHRL continues to apply, alongside IHL which is considered as *lex specialis*. In the context of Gaza, Israel's cyber espionage enabled targeting must be also assessed under Article 6 of the ICCPR. The essential legal question is whether the killings

[364] See more at: Office of the United Nations High Commissioner for Human Rights. (2024, December 31). *Pattern of Israeli attacks on Gaza hospitals raises grave concerns: Report*. Retrieved from: https://www.ohchr.org/en/press-releases/2024/12/pattern-israeli-attacks-gaza-hospitals-raises-grave-concerns-report

[365] Associated Press. (2024, August 10). *Israeli airstrike on a Gaza school used as a shelter kills at least 80, Palestinian officials say*. Retrieved from: https://apnews.com/article/israel-palestinians-hamas-war-10-august-2024-f33867d7596ebb70c1cb3a77fd4437cc

[366] Human Rights Watch. (2024, April 4). *Gaza: Israeli strike killing 106 civilians an apparent war crime*. Retrieved from: https://www.hrw.org/news/2024/04/04/gaza-israeli-strike-killing-106-civilians-apparent-war-crime

enabled by cyber espionage were "arbitrary," meaning that they are not permissible, necessary, or proportionate in pursuit of a legitimate military goal.

When looking at IHRL, the intentional use of force is a very extreme measure that is only allowed in a few circumstances. Killings that breach IHL, such as purposeful attacks on civilians, are also considered arbitrary under IHRL. However, it is important to maintain that in the context of active hostilities, IHL remains the *lex specialis*.[367]

To further clarify this, the Human Rights Committee's General Comment No. 36 on Article 6 of ICCPR has stressed this point, noting that the right to life is a fundamental right that always applies, including during armed conflicts and even when there are public emergencies. The Committee also highlighted that IHL and IHRL are two complementary bodies of law, and that compliance with IHL does not free a state of its responsibilities under IHRL.[368]

Therefore, Israel's use of cyber espionage tools like Lavender, in which thousands of people in Gaza are algorithmically identified for fatal targeting based on unverifiable or biased indicators, demonstrates a targeting technique that lacks transparency, human control, and tailored suspicion. These errors in due diligence, together with the enormous number of civilian victims, justify the conclusion that such executions do not just violate core IHL principles, but are also arbitrary deprivation of life under Article 6 of the ICCPR.

In conclusion, incorporating cyber espionage tools such as Lavandar and the Gospel into targeting proved that it did not minimize civilian injury. That is because, instead, by permitting fast, and large-scale strikes, it frequently increased harm and contributed to disproportionate consequences. When looking at the principles of IHL, it is clear that any foreseeable civilian losses must not be excessive in relation to concrete military gain. However, on the ground, there are several examples where many civilian lives of civilians were damaged for what Israel had claimed to be a military advantage, without providing clear evidence. Therefore, this constitutes a violation of the proportionality customary rule. This also constitutes a violation of the right to life enshrined in Article 6 of ICCPR. In addition, this ultimately violates Articles

[367] See supra note 302.

[368] See more on paragraphs 2,12,13, and 64 of the Human Rights Committee General Comment No. 36. Human Rights Committee. (2018). *General Comment No. 36 on Article 6 of the International Covenant on Civil and Political Rights, on the right to life* (CCPR/C/GC/36). United Nations. Retrieved from: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-36-article-6-right-life

27[369], 32[370], 33[371], and 147[372] of the GCIV.[373] It could also amount to a war crime in accordance with Article 8(2)(b)(iv) of the Rome Statute[374].[375]

Thus, after concluding that Israeli use of cyber espionage as a military tool in Gaza fails to comply with the principle of proportionality under IHL and subsequently the right to life under IHRL, the next section examines Israel's compliance with the principle of precaution.

5.3.2 Precautions in Cyber Espionage Enabled Targeting

In addition to prohibiting purposeful or disproportionate attacks on civilians, IHL also requires attackers to take all reasonable steps to reduce civilian casualties. Customary IHL Rule 15 states that "in the conduct of military operations, constant care must be taken to spare the civilian population, civilians and civilian objects. All feasible precautions must be taken to avoid, and in any event to minimize, incidental loss of civilian life, injury to civilians and damage to civilian objects."[376] This is also supported by Article 57 of AP I.[377] However, in the context in Gaza, the use of cyber espionage and automation that was allegedly intended to improve precision, as a type of precaution, but it usually resulted in fewer effective measures.[378] Automated targeting methods allowed a faster rate of attack, where precautionary checks that a fully human-driven process contains were absent.

---

[369] Article 27 of the Fourth Geneva Convention states that "Protected persons…shall be protected especially against all acts of violence or threats thereof…"
[370] Article 32 of the Fourth Geneva Convention states that it prohibits "measures of brutality whether applied by civilian or military agents…."
[371] Article 33 of the Fourth Geneva Convention states that "No protected person may be punished for an offence he or she has not personally committed. Collective penalties and likewise all measures of intimidation or of terrorism are prohibited. Pillage is prohibited. Reprisals against protected persons and their property are prohibited."
[372] Article 147 of the Fourth Geneva Convention lists grave breaches, including "willful killing," "torture or inhuman treatment," and "extensive destruction… not justified by military necessity."
[373] See supra note 191.
[374]Article 8(2)(b)(iv) of the Rome Statute states that "Intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated;" is a war crime.
[375] See supra note 315.
[376] International Committee of the Red Cross. (n.d.). *Rule 15. Principle of Precautions in Attack*. Customary IHL Database. Retrieved from: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule15
[377] See more at: International Committee of the Red Cross. (2006). *A guide to the legal review of new weapons, means and methods of warfare: Measures to implement Article 36 of Additional Protocol I of 1977*.
[378] See more at: Burke, G., & Mednick, S. (2025, February 18). *As Israel uses US-made AI models in war, concerns arise about tech's role in who lives and who dies*. Associated Press. Retrieved from: https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108

One key precautionary method that is outlined in Customary IHL Rule 16 is that is required target verification, which is needed because it ensures that the intended target is a legitimate military purpose rather than a civilian one.[379] This was also articulated in Article 57(2)(a)(i) of AP I.[380] With cyber espionage, verification sometimes ends at the digital profile. For example, in late 2023, the Israeli army deliberately divided Gaza into hundreds of cells on a map and tracked how many phones moved out of each place to assess compliance with evacuation orders. Therefore, if a zone had few active phones, the military assumed it was "evacuated" and safe to strike. This method is inherently inaccurate and prone to error. That is especially true because Israel deliberately cut off power disruptions which left many phones turned off or uncharged.[381] Therefore, using such an untrustworthy proxy, which is phones, to detect human presence without further human intelligence or any confirmation falls short of taking all feasible precautions to verify the target's identity. It suggests a lack of proper precautions, as the law of war necessitates.

Thus, one of the most pressing challenges is the reliance on AI-powered systems for target identification. The Israeli military, when using systems like "Lavender" and "The Gospel" to process massive volumes of data and compile lists of probable targets, may function with no human control, resulting in quick targeting decisions without sufficient verification.

Another cautious measure that needs to be taken into account by any attacker is the proper selection of weaponry and time to reduce harm, which was articulated in Customary IHL Rule 17.[382] This was also articulated in Article 57(2)(a)(ii) of AP I.[383]That means that attackers must choose an attack time that minimizes civilian risk and to cancel if the target does not meet expectations. With drones providing near-total ISR (intelligence, surveillance, and reconnaissance) coverage, the Israeli army could conceivably wait for a target to relocate to a less crowded area or strike when there are fewer civilians present.

However, for instance, the Israeli military's recent bombings on Gaza schools, particularly the ones that are being used as shelters for displaced civilians, shows a certain pattern. In a recent

[379] International Committee of the Red Cross. (n.d.). Rule 16. Target Verification. Customary International Humanitarian Law. Retrieved from: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule16
[380] See supra note 313.
[381] See supra note 165.
[382] International Committee of the Red Cross. (n.d.). *Rule 17. Choice of Means and Methods of Warfare*. Customary International Humanitarian Law. Retrieved from: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule17
[383] See supra note 313.

UN report, it was estimated that 95% of the schools in Gaza currently have structural damage. In addition, the report showed that a "direct hit" struck approximately 400 schools.[384] On the other hand, the Israeli forces said that Hamas operatives were using these schools for military reasons.[385] However, in most situations, like shown in earlier examples, no real evidence has been given to back these claims. What is important to highlight is that even if such a military presence is proven, releasing explosive weapons into densely populated displacement centers violates the need to take all reasonable care to reduce civilian injury.

Furthermore, three Israeli military sources said recently that the Israeli military has classified places like schools, hospitals, and municipal buildings as "heavy centers" especially over the last two months, because they say that they are being used by “Hamas terrorists” in addition to having civilians. According to the sources, attacks were authorized on such sites with only low-ranking “terrorists present”, even though people could be killed.[386]

Moreover, Israel uses warning measures in Gaza, like the "knock on the roof" strikes[387], SMS alerts, and mass evacuation orders[388]. However, these practices must also be looked at in the context of Israel's strong cyber espionage and surveillance capabilities, which support the delivery and monitoring of such warnings. Due to these capabilities, Israeli forces can follow the movements of people. This technological ability, even though it could apparently look like it is used to improve precision in attacks and to prevent civilian injury, also questions the effectiveness and good faith of these evacuation warnings.[389]

---

[384] United Nations Office for the Coordination of Humanitarian Affairs. (2025, May 9). *Verification of damages to schools based on proximity to damaged sites – Gaza, Occupied Palestinian Territory, Update #9*. ReliefWeb. Retrieved from: https://reliefweb.int/report/occupied-palestinian-territory/verification-damages-schools-based-proximity-damaged-sites-gaza-occupied-palestinian-territory-update-9-may-2025

[385] See more at: Davies, H. (2025, June 2). *Israeli strikes on Gaza schools used as civilian shelters are part of deliberate strategy, say sources*. The Guardian. Retrieved from: https://www.theguardian.com/world/2025/jun/02/israel-strikes-gaza-schools-strategy

[386] *Ibid*.

[387] See more at: France 24. (2021, May 20). *'Roof knocking': Israel warning system under scrutiny in Gaza conflict*. France 24. Retrieved from: https://www.france24.com/en/live-news/20210520-roof-knocking-israel-warning-system-under-scrutiny-in-gaza-conflict

[388] Fabian, E. (2024, May 6). *IDF using flyers, text messages and phone calls to instruct Gazans on evacuation of Rafah neighborhoods*. The Times of Israel. Retrieved from: https://www.timesofisrael.com/liveblog_entry/idf-using-flyers-text-messages-and-phone-calls-to-instruct-gazans-on-evacuation-of-rafah-neighborhoods/

[389] See supra note 165.

Warnings of civilians that could be affected by any attacks, in effective ways, are required under IHL, especially in Article 57(2)(c) of AP I[390] and Customary IHL Rule 20[391]. However, what is important about the warnings is that they must be relevant, offering civilians a real chance to avert danger. In the context of Gaza, this condition was recurrently not met. For instance, when the widely publicized order to evacuate 1.1 million people from northern Gaza, which was monitored via cyber espionage tools such as phone data tracking and geolocation, was not also accompanied by safe evacuation. Many civilians were not able to flee because of medical issues, a shortage of fuel, or the fear of being targeted while on the way as has happened before. Israeli officials were most likely aware of these limits via the same monitoring tools that influenced their targeting. In a specific example, on October 13, 2023, following the evacuation order, Israeli airstrikes targeted convoys of fleeing civilians. These attacks killed at least 70 people, including women and children, and injured over 200 others. The strikes took place on Salah al-Din Road, which Israel had designated as a "safe corridor" for evacuation. Therefore, such actions show a failure to take the needed precautions to spare civilian lives.[392]

In addition to the need for precautionary measures, collective punishment is also prohibited by Article 33 of the GCIV[393] and Customary IHL Rule 103[394]referred to it earlier. In the case of Gaza, the widespread distribution of evacuation orders for over one million individuals at once, which are then followed by attacks on what Israel designated as "safe corridors," raises questions. For example, the incident of October 13, 2023, described earlier reflects a punitive strategy to punish the civilian population as a whole.

What further adds onto this are the statements from high-ranking Israeli officials that suggest a desire to do broad harm and to punish the civilians. For instance, on November 18, 2023, Defense Minister Yoav Gallant declared that, referring to the civilian populations, “soon they'll realize the IDF's power, even in the southern part [of Gaza]" he added: "Those who were on the western side of Gaza City understand this well and have already met the deadly power of the IDF, those who are on the eastern side understand this tonight and will understand it in the

[390] See supra note 313.
[391] International Committee of the Red Cross. (n.d.). *Rule 20. Advance Warning*. Customary International Humanitarian Law. Retrieved from: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule20
[392] Sherlock, R., Wood, D., & Bashir, A. B. (2023, November 17). *Israel told Palestinians to evacuate to southern Gaza — and stepped up attacks there*. NPR. Retrieved from: https://www.npr.org/2023/11/17/1213579692/israel-gaza-evacuation-south-attacks
[393] See supra note 180.
[394] See supra note 339.

coming days, and those who are in the south of the Gaza Strip will also understand this soon."[395] Furthermore, National Security Minister Itamar Ben-Gvir stated that "as long as Hamas does not release the hostages it is holding, the only thing that needs to enter Gaza is hundreds of tons of explosives by the Air Force, and not an ounce of humanitarian aid."[396] When such statements, and many others, are evaluated alongside military activities, then such statements reflect a tactic that intends to harm civilians indiscriminately, which aligns with the notion of collective punishment.

Therefore, these actions only call into question the rules of precaution and proportionality in IHL, which contain aspects of collective punishment. The persistent panic created by mass evacuation orders, the threat or actual occurrence of strikes in designated "safe zones,", and the overriding Israeli narrative of broad retribution all contribute to a climate of terror among citizens. When this climate of fear and pain is purposely created, it emphasizes the gravity of the situation and the possibility for violations of international legal rules.

In conclusion, the cyber espionage enabled military actions in Gaza fail to meet the criterion of taking all the feasible precautions to protect civilians in Gaza. No state publicly confesses to breaking this requirement, instead, they claim consistent compliance with IHL. For example, an Israeli military spokesperson declared that the Israeli forces "operate exclusively on the grounds of military necessity and strictly in accordance with international law." However, the behavior observed on the ground in Gaza, especially in the use of cyber espionage-driven targeting completely contradicts such assurances. In addition, when civilians are subjected to recurrent displacement, targeted in what was declared by Israel to be safe zones, and made to live under constant threat and psychological stress, the harm appears to be indiscriminate and punitive in nature. In this situation, the systematic use of fear, deprivation, and unremitting violence against civilians may constitute collective punishment, which is clearly prohibited by Article 33 of the Fourth Geneva Convention and Customary IHL Rule 103.

As a result, this cyber espionage enabled activities to fail the precautionary test and run the possibility of becoming a grave violation of IHL by collectively punishing the Gaza civilian

[395] Law for Palestine. (2024, February 27). *Database of Israeli incitement to genocide, including after ICJ order*. Retrieved from: https://law4palestine.org/wp-content/uploads/2024/02/Database-of-Israeli-Incitement-to-Genocide-including-after-ICJ-order-27th-February-2024-.pdf
[396] *Ibid*.

population. This could also amount to war crimes as it could violate Article 8(2)(b)(iv) of the Rome Statute.[397]

Thus, this chapter showed in detail how Israeli cyber espionage creates major legal issues based on key IHL principles. Firstly, it shows how cyber espionage-based targeting usually fails to meet the principle of distinction because it depends on ambiguous or biased indicators and has resulted in sometimes deliberate civilian casualties. Similarly, the principle of proportionality is also violated when AI-generated intelligence leads to attacks that do more harm than any expected military advantage. This also violates the right to life that is protected under IHRL. The principle of precaution is also violated when the process of designating targets lacks transparency, human control, or clear guarantees against civilian harm. The chapter also shows that the violation of these principles could amount to war crimes and/or crimes against humanity under international criminal law.

Finally, this chapter finds that Israeli cyber espionage in Gaza, when used to lead or justify lethal operations, serves as part of a larger targeting infrastructure that typically violates IHL core principles of distinction, proportionality, and precautions. Even though even though this chapter focused primarily on IHL due to the context of active hostilities, it is important to stress that this does not preclude violations of IHRL. As in the West Bank, fundamental rights such as privacy and freedom of expression are also undermined by these practices, reaffirming the need to assess Israel's conduct under both IHL and IHRL in the occupied Palestinian territory.

[397] See supra note 315.

Chapter Six: Conclusion and Recommendations

6.1 Conclusion

"We are building the greatest weapon for oppression in the history of man, yet its directors exempt themselves from accountability."— Edward Snowden

This thesis sought to answer a critical and very pressing legal question: Is Israeli cyber espionage against civilians in the Occupied Palestinian Territory permissible under international law? It is a question that sits at the crossroads of massive technical growth, military dominance, and the shifting borders of international law. As Snowden's statements highlight, the issue is not just about the development of strong means of monitoring and control, but it is also linked to the impunity with which they are used. This is especially true in the case of the oPt, where Israel, acting as an occupying power, has used a large set of cyber espionage tools with what seems to be impunity.

This thesis concludes that Israel's cyber espionage practices in the oPt violate both IHRL and IHL. To specifically answer the research question, the thesis began by taking a close look at the historical development of espionage. It showed that, even though the practice of espionage is ancient, there have not been explicit restrictions under international law. Even as international legal frameworks have evolved, espionage in wartime is viewed with doubt, as it is recognized as a valid tactic, but can be punished under domestic law if the spy was caught, and the spy then loses the protection offered to them as civilians. On the other hand, espionage in peacetime is still in a legal vacuum. When assessing this in terms of the situation in the oPt, it appears to be in a legal gray zone, as it is neither a traditional wartime, nor is it in real peace.

Afterwards, the thesis gave a detailed historical analysis of Israel's intelligence system, which shows the long institutional track record of spying against Palestinians, as it extends back to the pre-state era. From the Haganah's clandestine units to the founding of Shin Bet, Mossad, Aman, and then specialized units like Unit 8200 and Mista'arvim, espionage has been embedded in the Israeli system. Over time, these classical espionage tools evolved and interacted with the digital revolution that occurred around the world, to create one of the world's most technologically advanced surveillance regimes.

As the entire world entered the digital age, Israel emerged as an upfront cyber power. This thesis explains how Israel rose to be a dominant player in the cyber world. It then explains the

tools and the deployment of Israel's systematic use of cyber espionage methods in the oPt, differentiating between the West Bank and the Gaza Strip. In the West Bank tools such as Pegasus spyware, facial recognition technologies like Blue Wolf and Red Wolf, AI-driven metadata analysis, predictive policing algorithms for social media monitoring, and surveillance UAVs seem to be used to gain control and overpower the civilian population. Meanwhile, in Gaza, AI tools such as Lavender, the Gospel, Where's Daddy and UAVs used for digital monitoring as tools of cyber espionage and even used for lethal operations seems to be used to locate and eliminate targets, often using lethal force. The thesis discovered that this cyber weaponry is more than just monitoring, as it is centered and purposeful intelligence operations aiming at achieving absolute informational supremacy over a civilian population living under occupation.

When the legality of these cyber espionage tools in the West Bank is analyzed, the thesis first takes a closer look at the dual framework of both IHRL and occupation law applicable and then uses them to analyze the situation. In terms of IHRL, it starts with the right to privacy and data protection, as it is concluded that cyber espionage tools and practices used by Israel, especially those examined, which are Pegasus spyware, facial recognition systems like Blue Wolf and Red Wolf, social media mass monitoring, and surveillance UAVs, are arbitrary and disproportionate intrusions on privacy that cannot seem to be justified under the ICCPR provisions or the standards that it sets for both necessity and proportionality. Since children as a vulnerable group are also impacted by these violations, this in turn also disregards the additional layer of protection afforded to them under ICCPR and CRC.

The thesis then examines the right to free expression and participation, concluding that the surveillance and punishment of political speech on social media, facilitated by the examined cyber espionage tools, significantly violates civic space and criminalizes dissent. The right to non-discrimination is also assessed, with evidence indicating a racially targeted monitoring system that is examined is used almost exclusively at Palestinians, which violates both IHRL and the principles of equality. After that, the chapter also assesses if such cyber espionage tools amount to collective punishment under IHL. The thesis finds that some tools used by Israel like the surveillance UAVs, seem to be related to collective punishment.

On a very important note, the thesis did not just investigate the act of using cyber espionage, but also the legal implications of how the data gathered is being used. It highlights how information obtained through the examined cyber espionage tools directly results in arbitrary

arrests and administrative detention based on vague suspicion profiles. The thesis then looks at how the cyber espionage data is also being used for coercion and to blackmail Palestinians to become informants, as it invades their private personal information and uses them against them. This violates the legal protections against coercion. Finally, it also shows how cyber espionage tools used in the West Bank can also directly support targeted force, including extrajudicial killings, which fail to meet the legal threshold for the use of lethal force under IHRL.

All these findings lead to the fact that Israeli cyber espionage in the West Bank is more than just an intelligence collection tool, as it is used as a key component of a digital occupation system, and it even weaponizes the data gathered to suppress an occupied population, which violates many principles under international law.

The thesis then shifts its focus on the cyber espionage tools used specifically in Gaza, where they have been directly used with greater military practice and more lethal effects. It first shows how the legal framework in Gaza varies from the West Bank, as IHL prevails in times of active hostilities. In such context, IHL allows for specific targeting tools, however, despite this, this thesis discovers that Israel's use of cyber espionage tools in Gaza regularly violates the key IHL customary principles of distinction, proportionality, and precaution.

Israel has been using a system of quick, high-volume targeting by integrating cyber intelligence with AI-based systems like "Lavender." Some may blame the mass targeting on technological errors or issues, such as algorithmic misclassification or automation bias, the thesis argues that the root cause is deliberate Israeli policy rather than technical malfunction, even though malfunctions can still occur. According to testimony from Israeli intelligence officials and statements by government officials, the system is purposely designed to decrease the threshold for fatal targeting. The concept of distinction is thus deliberately violated as civilian profiles are flagged algorithmically with little or no human verification. The principle of proportionality is also violated when entire apartment blocks are destroyed to kill a single individual. This in turn also violates the right to life protected under IHRL. These conclusions are reinforced by open-source research and by confessions made within the Israeli military officers during the current active hostilities that started in 2023.

On an important note, when cyber espionage enabled targeting and attacks are carried out against individuals who do not pose an imminent threat, or when such operations result in widespread civilian harm, often based on vague algorithmic discriminatory assessments, the

thesis finds that these acts may not only be illegal under IHRL and IHL, but may also constitute war crimes and crimes against humanity. This argument is directly supported by official findings that show that systematic attacks on civilians, destruction of protected infrastructure, and the excessive use of force are severe violations of international criminal law. Therefore, when cyber espionage is the foundation for such attacks, then it is incorporated into a larger machinery of violence that fits the criteria for international crimes.

Therefore, looking deeply to all the findings, from the historical examination of Israel's espionage practices dating back to the pre-state era, through the establishment of formal intelligence institutions that conducted traditional espionage, and closing with Israel's rise as a leading cyber power deploying advanced cyber espionage tools against Palestinian civilians, it is clear that these techniques represent a continuous trend of increasingly sophisticated espionage and control.

Thus, this all can also reflect a dangerous worldwide precedent, which is that cyber espionage is now being normalized as a tool of war, mass surveillance, and control, one that avoids transparency, accountability, and legal constraints. Looking back at Snowden's warning stated earlier, it must be acknowledged that the creation of these "weapons for oppression" is not limited to a single state's regime. This thesis focuses only on Israel's use of cyber espionage during the context of occupation. However, it is very important to put this in the larger context where somewhat similar methods are used in different parts of the world. For instance, by Israel's allies, particularly the United States. Snowden's comment came in the context of mass surveillance revelations by the US against Americans, as the US government's use of many cyber espionage tools was criticized for gathering and analyzing data on millions of citizens, even including foreigners, with little supervision. Like the Israeli case, these activities were justified using national security and counterterrorism rhetoric, but it is at the expense of rights, dignity, and democratic accountability.

As a result, while this thesis focuses on a specific situation, the ramifications are much wider. The normalization of the use of cyber espionage in the context of occupation serves as a warning for other contexts of armed conflicts, and even in peacetime.

These findings highlight the urgent need for legal and policy responses, both to address the specific violations identified in this case and to strengthen international protection against

similar practices elsewhere. The following section provides concrete recommendations to that end.

6.2 Recommendation

The findings of this thesis highlight the urgent need for international legal reform and to have more credible enforcement mechanisms as there is a visible growing use of cyber espionage and digital targeting in modern warfare. At the moment, there is a significant regularizing gap in international law, which is that the rapid advancement of digital technologies, especially in the fields of surveillance, AI, and metadata analysis, has far outpaced the legal frameworks that are designed to regulate hostilities and thus protect civilians. Both IHL and IHRL, in addition to international criminal law and other areas of international law, were all created before the development of cyberspace, predictive algorithms, and AI-powered targeting. Therefore, normally they provide only fragmented instructions for controlling cyber-based techniques used in armed conflicts. This legal gap has resulted in a permissive atmosphere in which new technologies are used with minimal oversight, which significantly affects the civilian populations.

However, what is essential to highlight is that the main issue goes way beyond just the lack of defined rules under international law. That is because even in areas where international law is very clear and properly or fully established, such as the prohibition on extrajudicial killings, or civilian protection, states continue to commit these violations. Thus, this shows that there is a larger structural issue rather than just the lack of international rule, which is that international law is shaped by principles, but it is implemented by political will. Therefore, having a selective application of international law, normally dictated by powerful states, has created an environment of major impunity, where political interests have power over international accountability institutions. Thus, in this context justice becomes conditional making law submissive to power. Therefore, real transformation requires more than just technical improvements to international law. It deeply needs the development of enforcement systems that are independent, consistent, and are capable of holding all international actors accountable, regardless of their political power. That is because it is obvious that without this type of accountability, digital warfare and the dangerous use of digital technologies in general will continue to expand as a tool of oppression, while international law will remain more aspirational rather than functioning.

To address all these fundamental issues, the international legal community must create enforceable legal norms designed very specifically to govern cyber espionage and digital targeting activities. This would need to include explicit definitions of cyber espionage, the situations under which digital monitoring may be used in different types of armed conflict including occupation, and how specifically algorithmic targeting needs to comply with the principles of distinction, proportionality, and precaution. Thus, international bodies like the International Committee of Red Cross (ICRC), the International Law Commission (ILC), different UN bodies, and panels made from legal experts should introduce a review process to codify these standards, based on the existing jurisprudence and new technical changes and developments.

In addition, a General Comment by the UN Human Rights Committee specifically on the Extraterritorial Application of the Right to Privacy in Conflict and Occupation Situations would also be a significant step forward. Even though General Comment No. 16 that was established in 1988, already laid down the critical understandings about the right to privacy under Article 17 of the ICCPR, it still came years before the digital age, therefore, and it does not explicitly mention cyber espionage technologies or extraterritorial data collecting. For instance, General Comment No. 36 (2018) successfully addressed the application of the right to life in the context of new technology, such as drones and other forms of remote targeting. Therefore, there seems to still be a significant gap in the right to privacy. Thus, a separate General Comment is required to clarify how Article 17 of the ICCPR applies extraterritorially, specifically in cases of different forms of armed conflict including occupation and considering the constantly evolving cyber espionage.

Second, and very importantly, enforcement must be reinvented in ways that would ensure that violations related to cyber technology are clearly met with the appropriate repercussions. Practical steps forward could be enhancing the International Criminal Court's (ICC) role in investigating and prosecuting cyber-enabled war crimes and crimes against humanity, such as targeted executions based on AI profiling or systematic surveillance of civilian populations. In addition to that, states must also be encouraged to use universal jurisdiction to pursue legal action against persons and entities involved in digital repression.

Third, tangible action needs to be taken to protect the rights of Palestinians and others under digital occupation. This could include assisting with the development of Palestinian digital infrastructure that would help in reducing the dependency and reliance on Israeli-controlled

networks. In addition, international organizations and civil society actors should provide more legal aid, and some more digital literacy initiatives. In addition, independent digital forensics teams should be formed to evaluate and investigate digital evidence in relation to Israeli targeting decisions and surveillance operations.

Finally, the international community needs to resist the normalization of this type of "cyber tyranny" and advocate for a worldwide response to the ethical and legal issues raised by digital warfare. Academic institutions, civil society organizations, and digital rights coalitions should focus on studies and advocacy efforts related to the relationship of cyber technology, armed conflict, and human rights. Importantly, whistleblower protections need to be strengthened for anyone in the military or technology sectors who report unlawful or unethical cyber practices. Therefore, transparency must be demanded from both governments and corporate players on the use of AI in both cyber espionage and in targeting.

This all could happen only with global effort to begin to reverse the entrenchment of impunity and recover international law as a legitimate safeguard against state violence in the digital age.

References

American Public University. (n.d.). What is HUMINT and how is it used in the intelligence field?

National Security Agency. (n.d.). Signals Intelligence (SIGINT) Overview.

U.S. Department of Defense. (1991). Joint Publication 3-54: Joint Doctrine for Operations Security.

7amleh – The Arab Center for the Advancement of Social Media. (2023, December). Israel's Surveillance Industry and Human Rights.

Abraham, Y. (2024, April 3). 'Lavender': The AI machine directing Israel's bombing spree in Gaza. +972 Magazine.

Abraham, Y. (2024, April 3). 'Lavender': The AI machine directing Israel's bombing spree in Gaza. +972 Magazine.

Abreu, M. (2025, March 27). "Where international law goes to die": Mechanisms blocking justice for journalists and civil society [Gaza Project]. Forbidden Stories.

Abreu, M., Delpuech, A., & Layan, E. (2024, June 25). Death from Above: How Israeli Drones are Killing Journalists in Gaza. Arab Reporters for Investigative Journalism.

Abreu, M., Delpuech, A., Layan, E., Batrawi, W., Rueckert, P., Jurado, S. Á., Youssef, Y., Osman, H., Abraham, Y., Carpentier, A., & Zerrouky, M. (2024, July 25). Death from above: How Israeli drones are killing journalists in Gaza. Arab Reporters for Investigative Journalism (ARIJ).

Addameer Prisoner Support and Human Rights Association. (2016, July). Administrative detention in the occupied Palestinian territory: A legal analysis report.

Addameer Prisoner Support and Human Rights Association. (2018, October). Arrests on charges of "incitement" on social media platforms and Israeli government policy: A Facebook case study.

Al Jazeera Media Network. (2023, December 15). Al Jazeera condemns Israeli forces killing of cameraman Samer Abudaqa. Al Jazeera.

Al Jazeera Media Network. (2023, October 25). Al Jazeera condemns killing of journalist Wael Al-Dahdouh's family in Gaza. Al Jazeera.

Al Jazeera. (2015, November 13). Israeli army unit Storms Hospital and kills Palestinian. Al Jazeera.

Al Jazeera. (2022, August 7). Timeline: Israel's attacks on Gaza since 2005.

Al Jazeera. (2022, February 8). Israeli soldiers open fire at car in Nablus killing Palestinians.

Al Jazeera. (2023, December 17). Israeli military uses drones to kill Palestinians in West Bank's Tulkarem

Al Jazeera. (2023, June 21). Israel launches air strike in West Bank, killing three Palestinians.

Al Jazeera. (2025, May 8). Israel retrofitting DJI commercial drones to bomb and surveil Gaza.

Aldrich, R. J. (2001). The UK, the USA, and the Internet: The Politics of Intelligence Sharing. Review of International Studies, 27(3), 405–428.

Al-Haq. (2019). Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.

Al-Haq. (2021, November 1). Designated shrinking space: Israel's systematic harassment of Palestinian civil society organizations [Briefing paper]. Al-Haq.

Al-Haq. (2022, March 3). Urgent Appeal to the United Nations Special Procedures on the Extrajudicial Execution and Wilful Killing of Palestinians Mr. Ashraf Mubaslat, Mr. Mohammad Dakhil, and Mr. Adham Mabrukah, by the Israeli Occupying Forces on 8 February 2022 in Nablus, West Bank.

Almutawa, A., & Walker, C. (2024). Chilling effects of surveillance and human rights. Journal of Human Rights Practice, 16(1), 397–412.

American Civil Liberties Union. (2014). Privacy rights in the digital age: A proposal for a new General Comment on the right to privacy under Article 17 of the International Covenant on Civil and Political Rights.

American-Israeli Cooperative Enterprise. (n.d.). Hashomer. Jewish Virtual Library.

Amnesty International. (2009). Israel/Gaza: Operation 'Cast Lead': 22 days of death and destruction (MDE 15/007/2009).

Amnesty International. (2017, June 5). Israel's occupation: 50 years of dispossession.

Amnesty International. (2021). Forensic methodology report: How to catch NSO Group's Pegasus.

Amnesty International. (2021, June 24). Israeli police targeted Palestinians with discriminatory arrests, torture and unlawful force.

Amnesty International. (2021, November 8). Devices of Palestinian human rights defenders hacked with NSO Group's Pegasus spyware.

Amnesty International. (2023, May 2). Automated apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT.

Amnesty International. (2023, November 8). Israel/OPT: Horrifying cases of torture and degrading treatment of Palestinian detainees amid spike in arbitrary arrests.

Amnesty International. (2024, December 5). Amnesty International concludes Israel is committing genocide against Palestinians in Gaza.

Andrew, C. (n.d.). The later Cold War. Security Service M15.

Anera. (2024, May 6). 7 months of war on Gaza: A timeline of events and humanitarian response.

AP News. (2024, November 24). Israel detains Palestinians over social media posts amid Gaza war.

Army Recognition. (2024, April 9). Israel strengthens aerial capabilities with new Hermes 900 Star drone squadron. Defense News Army 2024.

Associated Press. (2021, November 11). Palestinians say Israel hacked officials' phones with Pegasus.

Associated Press. (2024, August 10). Israeli airstrike on a Gaza school used as a shelter kills at least 80, Palestinian officials say.

Baker, K. (2025, January 16). Cyber Espionage Explained. CrowdStrike. , Brown, G. (2015). Spying and fighting in cyberspace: What is which. J. Nat'l Sec. L. & Pol'y, 8, 621.

Banks, W. C. (2016). Cyber espionage and electronic surveillance: Beyond the media coverage. Emory LJ, 66, 513.

Banks, W. C. (2017). Cyber Espionage and International Law. Emory Law Journal, 66(3), 527–573.

Beaumont, P. (2014, September 12). Israeli intelligence veterans refuse to serve in Palestinian territories. The Guardian.

Beaumont, P. (2021, November 5). Israel escalates surveillance of Palestinians with facial recognition program in West Bank. The Washington Post.

Beim, J. (2018). Enforcing a prohibition on international espionage. Chicago Journal of International Law, 18(2).

Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F., & Scherrer, A. (2013). Mass surveillance of personal data by EU member states and its compatibility with EU law. Liberty and Security in Europe Papers, (61).

Black, I. (1987). The origins of Israeli intelligence. Intelligence and National Security, 2(4), 151–156.

Black, I., & Morris, B. (1991). Israel's Secret Wars: A History of Israel's Intelligence Services (pp. 89–92). New York: Grove Weidenfeld.

Bregman, A. (2023, October 26). A little history of Shin Bet. Engelsberg Ideas.

Brehm, M. (2020). Freedom of assembly under attack: General comment No. 37 and interference through surveillance and internet shutdowns. International Review of the Red Cross, 102(913), 145–170.

B'Tselem & Palestinian Centre for Human Rights. (2021, December). Unwilling and Unable: Israel's Whitewashed Investigations of the Great March of Return Protests.

Buchan, R. J. (2016). The international legal regulation of cyber espionage. Tallinn Papers, 65-86.

Burke, G., & Mednick, S. (2025, February 18). As Israel uses US-made AI models in war, concerns arise about tech's role in who lives and who dies. Associated Press.

Chacar, H. (2023, October 20). Israeli police arrest Arab citizens expressing solidarity with Gaza. Reuters.

Chatelle, T. (2024, August 30). How Israel's Elite Intelligence Unit Targets Queer Palestinians in the West Bank. Drop Site News.

Chicago Journal of International Law. (2021). Rethinking espionage in the modern era. The University of Chicago.

Cohen, M. S., & Freilich, C. D. (2024). Israel: The Making of a Global Cyber Power.

Commission of Detainees and Ex-Detainees Affairs. (n.d.). Official website.

Committee to Protect Journalists. (2023, December 15). Samer Abu Daqqa. CPJ.

Coop, S. (2024). The Israel-Palestine conflict from the perspective of international humanitarian law (Expert Comment No. 2024-11). Japanese Society of International Law.

Council on Foreign Relations. (n.d.). What is intelligence?. CFR Education.

CrowdStrike. (2025, January 16). Cyber Espionage Explained.

Cyber Risk GmbH. (n.d.). From espionage to cyber espionage.

Dannies, K. (2016). Charles Boutagy and the Nili Network during World War I. Jerusalem Quarterly, (63). Institute for Palestine Studies.

Davies, H. (2025, June 2). Israeli strikes on Gaza schools used as civilian shelters are part of deliberate strategy, say sources. The Guardian.

Davies, H., & Abraham, Y. (2025, March 6). Revealed: Israeli military creating chatgpt-like tool using vast collection of Palestinian surveillance data. The Guardian.

Davies, H., McKernan, B., & Trew, B. (2023, December 1). 'The Gospel': How Israel uses AI to select bombing targets. The Guardian.

Deeks, A. (2024, October 21). Using artificial intelligence in warfare creates constitutional concerns, argues professor. University of Virginia School of Law.

Defense for Children International – Palestine. (2024, August 29). Israeli drone strike kills Palestinian brothers in massive northern West Bank incursion.

Defense for Children–International Palestine. (2025, February 3). Israeli drone strike kills 14-year-old Palestinian boy in Jenin. Defense for Children Palestine.

Democracy Now! (2024, April 5). Lavender & Where's Daddy: How Israel used AI to form kill lists & bomb Palestinians in their homes.

Democracy Now! (2024, April 5). Lavender & Where's Daddy: How Israel used AI to form kill lists & bomb Palestinians in their homes.

Diamond, E., Nohle, E., & Schmidl, A.-C. (2025, January 30). The legal framework regulating Israel's use of force in the West Bank. Opinio Juris.

DIMSE. (n.d.). Skylark mini UAV. Defense & Intelligence Military Systems & Equipment (DIMSE).

Dwoskin, E. (2021, November 8). Israel escalates surveillance of Palestinians with facial recognition programs in the West Bank. The Washington Post.

Editorial Team. (2024, July 14). The Interplay of Espionage and Technology Advancements. Total Military Insight.

European Coordination of Committees and Associations for Palestine. (2014, January 29). Israel's obligations as an occupying power under international law, its violations and implications for EU policy.

European Court of Human Rights. (2006). Weber and Saravia v. Germany (dec.), Application No. 54934/00, Decision of 29 June 2006.

European Court of Human Rights. (2008). Liberty and Others v. the United Kingdom, Application No. 58243/00, Judgment of 1 July 2008.

Fabian, E. (2023, October 9). Defense minister announces 'complete siege' of Gaza: No power, food or fuel. The Times of Israel.

Fabian, E. (2024, May 6). IDF using flyers, text messages and phone calls to instruct Gazans on evacuation of Rafah neighborhoods. The Times of Israel.

Folsom, T. C. (2007). Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality). Tul. J. Tech. & Intell. Prop., 9, 75.

Forno, R. (2024, April 1). What is Volt Typhoon? A cybersecurity expert explains the Chinese hackers targeting US critical infrastructure. UMBC.

France 24. (2021, May 20). 'Roof knocking': Israel warning system under scrutiny in Gaza conflict. France 24.

France 24. (2024, February 6). West Bank Palestinians 'exhausted' by omnipresent Israeli surveillance. France 24.

Freilich, C., & Cohen, M. (2021). Israel: The Making of a Global Cyber Power. Oxford University Press.

Friedman, J. A., & Zeckhauser, R. J. (2018). Assessing uncertainty in intelligence. Intelligence and National Security, 33(2), 232–246.

Galpin, T. S. (2016). The difference between intelligence and espionage.

Garza, A. de la. (2019, September 5). The true story behind the spy on Netflix. Time.

Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War, art. 5, Aug. 12, 1949.

Global X ETFs. (2022, June 3). Cybersecurity in Israel: Fortifying digital defenses amid elevated risks.

Gomez, J., Martinez, L., & Crawford, S. K. (2023, November 14). US says it has intelligence Hamas has used Gaza's Al-Shifa Hospital to hold hostages. ABC News.

Gritten, D. (2023, June 22). Rare Israeli drone strike kills Palestinian militants in West Bank. BBC News.

Guardian News and Media. (2024, September 19). Hezbollah device blasts: How did pagers and walkie-talkies explode and what do we know about the attacks?. The Guardian.

Gunter, J. (2023, December 15). How Israel jails hundreds of Palestinians without charge. BBC News.

Gunter, J. (2023, December 15). How Israel jails hundreds of Palestinians without charge. BBC News Pidgin.

Gurijala, B. (2021, August 9). What is pegasus? how surveillance spyware invades phones. Scientific American.

Hague Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907.

Haque, A. A. (2024, December 12). The International Criminal Court's classification of armed conflicts in the situation in Palestine. Just Security.

Harel, A. (2017, May 31). How Israel jails Palestinians because they fit the 'terrorist profile'. Haaretz.

Hasson, N. (2020, December 31). Israel to fund drones, patrol units to monitor unauthorized Palestinian construction. Haaretz.

Helga Tawil-Souri. (2012). Digital Occupation: Gaza's High-Tech Enclosure. Journal of Palestine Studies, 41(2), 27–43.

Henckaerts, J.-M., & Doswald-Beck, L. (2005). Customary international humanitarian law: Volume I: Rules. International Committee of the Red Cross.

Hennigan, W. J. (2021, September 17). 'A Tragic Mistake.' Botched Drone Strike in Afghanistan Raises Concerns Over Biden's Counterterrorism Strategy. Time.

Human Rights Committee General Comment No. 36. Human Rights Committee. (2018). General Comment No. 36 on Article 6 of the International Covenant on Civil and Political Rights, on the right to life (CCPR/C/GC/36). United Nations.

Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (1988).

Human Rights Committee. (1994). Toonen v. Australia, Communication No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992.

Human Rights Committee. (2004, May 26). General comment No. 31: The nature of the general legal obligation imposed on States Parties to the Covenant (CCPR/C/21/Rev.1/Add.13). United Nations.

Human Rights Watch. (2019, December 17). Born without civil rights: Israel's use of draconian military orders to repress Palestinians in the West Bank.

Human Rights Watch. (2021, April 27). A threshold crossed: Israeli authorities and the crimes of apartheid and persecution.

Human Rights Watch. (2021, November 8). Spyware used to hack Palestinian rights defenders.

Human Rights Watch. (2022, June 14). Gaza: Israel's 'Open-Air Prison' at 15.

Human Rights Watch. (2023, February 2). Israel: Collective punishment against Palestinians.

Human Rights Watch. (2023, November 14). Gaza: Unlawful Israeli hospital strikes worsen health crisis.

Human Rights Watch. (2023, November 29). Why does Israel have so many Palestinians in detention and available for a swap?

Human Rights Watch. (2023, October 27). How does international humanitarian law apply in Israel and Gaza?

Human Rights Watch. (2024). Israel and Palestine. In World Report 2024.

Human Rights Watch. (2024, April 4). Gaza: Israeli strike killing 106 civilians an apparent war crime.

Human Rights Watch. (2024, May 8). West Bank: Israeli Forces' Unlawful Killings of Palestinians.

Human Rights Watch. (2024, September 10). Gaza: Israeli military's digital tools risk civilian harm.

Human Rights Watch. (2024, September 10). Questions and Answers on the Israeli military's use of digital tools in Gaza.

Human Rights Watch. (2024, September 10). Questions and answers: Israeli military's use of digital tools in Gaza.

Human Rights Watch. (2025, April 28). A hazard to human rights: Autonomous weapons systems and digital decision-making.

Hutchins, T. E. (2021). Maritime espionage and the legal consequences of the United States' potential ratification of the United Nations Convention on the Law of the Sea. National Security Law Journal, 8(1), 1–53.

ICJ, Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem, Advisory Opinion (2024).

ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, ICJ Reports 2004.

ICRC. (2024, September 4). The risks and inefficacies of AI systems in military targeting support. Humanitarian Law & Policy Blog.

Institute for Middle East Understanding. (2021, November 29). Fact sheet: Israeli surveillance & restrictions on Palestinian movement.

International Commission of Jurists. (2020, June). Israel: Ensure full compliance with the International Covenant on Civil and Political Rights [Advocacy Analysis Brief].

International Commission of Jurists. and United Nations Human Rights Committee. (2014, November 21). Concluding observations on the fourth periodic report of Israel (CCPR/C/ISR/CO/4). United Nations.

International Committee of the Red Cross (ICRC). (1949). Geneva Convention relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention).

International Committee of the Red Cross (ICRC). (1977). Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

International Committee of the Red Cross (ICRC). (n.d.). Rule 107. Spies. Customary IHL Database.

International Committee of the Red Cross (ICRC). (n.d.). Targeted killings. ICRC Casebook.

International Committee of the Red Cross. (1907). Hague Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. Articles 42–43.

International Committee of the Red Cross. (1949). Geneva Convention relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention). United Nations Treaty Series, vol. 75.

International Committee of the Red Cross. (1958). Commentary on the Fourth Geneva Convention: Relative to the Protection of Civilian Persons in Time of War. Geneva: International Committee of the Red Cross.

International Committee of the Red Cross. (1977). Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

International Committee of the Red Cross. (2006). A guide to the legal review of new weapons, means and methods of warfare: Measures to implement Article 36 of Additional Protocol I of 1977. Geneva: ICRC.

International Committee of the Red Cross. (2021). Artificial intelligence and machine learning in armed conflict: A human-centred approach. International Review of the Red Cross, 102(913), 463–479.

International Committee of the Red Cross. (2024, July 26). What does the law say about the responsibilities of the Occupying Power in the occupied Palestinian territory?

International Committee of the Red Cross. (n.d.). Lex specialis. ICRC Casebook.

International Committee of the Red Cross. (n.d.). Rule 1. The Principle of Distinction between Civilians and Combatants. Customary IHL Database.

International Committee of the Red Cross. (n.d.). Rule 103. Collective Punishments. In Customary International Humanitarian Law, Volume I: Rules.

International Committee of the Red Cross. (n.d.). Rule 15. Principle of Precautions in Attack. Customary IHL Database.

International Committee of the Red Cross. (n.d.). Rule 16. Target Verification. Customary International Humanitarian Law.

International Committee of the Red Cross. (n.d.). Rule 17. Choice of Means and Methods of Warfare. Customary International Humanitarian Law.

International Committee of the Red Cross. (n.d.). Rule 2. Violence aimed at spreading terror among the civilian population. Customary International Humanitarian Law.

International Committee of the Red Cross. (n.d.). Rule 20. Advance Warning. Customary International Humanitarian Law.

International Committee of the Red Cross. (n.d.). Rule 34. Denial of quarter and other forms of perfidy. In Customary IHL Database.

International Court of Justice. (2004). Legal consequences of the construction of a wall in the Occupied Palestinian Territory, Advisory Opinion.

International Court of Justice. (2024). Advisory Opinion on the Legal Consequences of Israel's Policies and Practices in the Occupied Palestinian Territory, including East Jerusalem.

International Court of Justice. (2024, April 30). Alleged breaches of certain international obligations in respect of the Occupied Palestinian Territory (Nicaragua v. Germany), Order on provisional measures.

International Court of Justice. (2024, July 19). Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem (Advisory Opinion).

International Court of Justice. (2024, July 19). Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem (Advisory Opinion).

International Court of Justice. (2024, July 19). Summary of the Advisory Opinion of 19 July 2024: Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem.

International Criminal Court, Pre-Trial Chamber I. (2021, February 5). Decision on the 'Prosecution request pursuant to article 19(3) for a ruling on the Court's territorial jurisdiction in Palestine (ICC-01/18-143).

International Criminal Court. (2011). Rome Statute of the International Criminal Court.

International Criminal Court. (2024, November 21). Situation in the State of Palestine: ICC Pre-Trial Chamber I rejects the State of Israel's challenges to jurisdiction and issues warrants of arrest for Benjamin Netanyahu and Yoav Gallant.

International Residual Mechanism for Criminal Tribunals. (2004.). Civilian population. ICTR/ICTY/IRMCT Case Law Database.

International Spy Museum. (n.d.). Espionage facts.

Interview with A.S., Jenin resident, May 2025. Name anonymized for security reasons.

Interview with H.T., Nablus resident, May 2025. Name anonymized for security reasons.

Interview with M.A., Ramallah resident, May 2025. Name anonymized for security reasons.

Interview with R.T., Ramallah resident, May 2025. Name anonymized for security reasons.

Interview with W.S., Jenin resident, May 2025. Testimony provided in Arabic and translated by the author.

Israel Defense Forces. (n.d.). Military Intelligence Directorate.

Israel Ministry of Foreign Affairs. (n.d.). Mossad – The Institute for Intelligence and Special Tasks.

Israel Security Agency. (n.d.). About the ISA.

Israeli Supreme Court. (2006, December 14). Public Committee Against Torture in Israel v. Government of Israel (HCJ 769/02).

Jerusalem Post. (2023, November 22). How Israel's Heron drone has changed the way the IDF fights wars. The Jerusalem Post.

Jewish Virtual Library. (n.d.). The Mossad.

Katibah, L. (2024, October). The genocide will be automated—Israel, AI and the future of war.

Kaye, D. (2019). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: Surveillance and human rights (A/HRC/41/35). United Nations Human Rights Council.

Kent, N. (2019). The secret world: A history of intelligence. The RUSI Journal, 164(1), 86–93.

Khosravi M, Zare Z, Mojtabaeian SM, Izadi R. Artificial Intelligence and Decision-Making in Healthcare: A Thematic Analysis of a Systematic Review of Reviews. Health Services Research and Managerial Epidemiology.

Kmiotek, C. (2024, October 29). Israel claims it is no longer occupying the Gaza Strip. What does international law say? Atlantic Council.

Kotliar, D. M., & Carmi, E. (2024). Keeping Pegasus on the wing: legitimizing cyber espionage. Information, Communication & Society, 27(8), 1499-1529.

La Rue, F. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/23/40). United Nations Human Rights Council.

Law for Palestine. (2024, February 27). Database of Israeli incitement to genocide, including after ICJ order.

Lebovic, S. (2023, November 26). The song and dance of American secrecy. Foreign Policy.

Lentin, R. (2017). Race and surveillance in the settler colony: the case of Israeli rule over Palestine. Palgrave Communications, 3(1), 1-10.

Leone, D. (2019, July 8). True story: What happened when the Soviet Union shot down Francis Gary Powers' U-2. The National Interest.

Levy, G. (2025, February 1). Israeli troops are now going through Palestinians' phones. Anything 'forbidden' provokes abuse. Haaretz.

Lierens, E. (2022, July 23). KGB: History, Structure and Operations. Grey Dynamics.

Lippert, K. J., & Cloutier, R. (2021). Cyberspace: A digital ecosystem. Systems, 9(3), 48.

Lubin, A. (2022). The rights to privacy and data protection under international humanitarian law and human rights law. In the Research Handbook on Human Rights and Humanitarian Law (pp. 462-491). Edward Elgar Publishing.

Luma-Osmani, S., CIVULI, A., ARIFI, G., & Rufati, E. (2022). Cyber espionage consequences as a growing threat. Journal of Natural Sciences and Mathematics of UT, 7(13-14), 13-20.

Lyon, D. (2001). Surveillance after September 11. Sociological Research Online, 6(3).

Malik, N. (2024, October 31). 'I couldn't cry over my children like everyone else': The tragedy of Palestinian journalist Wael al-Dahdouh. The Guardian.

Mandour, M. (2025, June 18). Attacks, arrests, threats, censorship: The high risks of reporting the Israel-Hamas war. Committee to Protect Journalists.

Matar, H. (2022, April 27). Nowhere to hide: The impact of Israel's digital surveillance regime on Palestinians. Middle East Institute.

McGreal, C. (2023, October 16). The language being used to describe Palestinians is genocidal. The Guardian.

Media Defence. (n.d.). The right to freedom of expression under international law. In Module 1: Key principles of international law and freedom of expression. Media Defence.

Mendel, Y., & Karkabi, N. (2023). The Re-Enchantment of the Orient: Mista 'arvim and Their Special Status in Jewish-Israeli Society. The Middle East Journal, 77(2), 161-180.

Middle East Eye. (2021, November 5). Israel can monitor every telephone call in West Bank and Gaza, says intelligence source.

Middle East Eye. (2024, November 13). Israeli army 'preparing for years-long presence in Gaza'. Middle East Eye.

Middle East Monitor. (2023, November 12). Anyone who supports Hamas should be eliminated: Israeli minister.

Middle East Monitor. (2023, October 29). Netanyahu declares holy war against Gaza, citing the Bible.

Mielko, T. (2023). Could Pegasus Gate have been prevented? The evolution of the export control regime for cyber-surveillance tools in Israel. Cybersecurity and Law, 9.

Nachinova, A. (2021). Facing the future: Emerging militarisation of facial recognition and public international law considerations (LL.M. Capstone Thesis, Central European University; Supervisor: T. Soave).

Nakashima, E., & Loveluck, L. (2024, January 3). U.S. 'confident' that Hamas used al-Shifa Hospital as command center. The Washington Post.

Nashif, N., & Fatafta, M. (2017). Surveillance of Palestinians and the fight for digital rights. Policy Brief, Al Shabaka, 23, 1-10.

Navarrete, I., & Buchan, R. (2018). Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions. Cornell International Law Journal, 51(3), 595–624.

NDTV News Desk. (2025, May 22). "Every baby in Gaza is an enemy": Ex-Israeli lawmaker's shocking remarks. NDTV.

New Arab. (2015). Mista'arvim: Israel's Notorious Undercover Agents.

Newsroom. (2025, June 6). 226 journalists killed in Gaza by Israeli army since Oct. 7: Gaza Media Office. Türkiye Today.

O'Connor, N. (2013, February 19). Gay Palestinians are being blackmailed into working as informants. VICE.

Office of the Director of National Intelligence. (2024, March 8). The IC OSINT Strategy 2024–2026.

Office of the High Commissioner for Human Rights. (2024, July 19). UN experts hail ICJ declaration on the illegality of Israel's presence in the Occupied Palestinian Territory.

Office of the United Nations High Commissioner for Human Rights. (2021, October 26). Israel's "terrorism" designation an unjustified attack on Palestinian civil society – Bachelet.

Office of the United Nations High Commissioner for Human Rights. (2014). The right to privacy in the digital age (A/HRC/27/37). United Nations Human Rights Council.

Office of the United Nations High Commissioner for Human Rights. (2014). The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37). United Nations.

Office of the United Nations High Commissioner for Human Rights. (2020). Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests (A/HRC/44/24). United Nations Human Rights Council.

Office of the United Nations High Commissioner for Human Rights. (2021, October 26).

Office of the United Nations High Commissioner for Human Rights. (2024, December 31). Pattern of Israeli attacks on Gaza hospitals raises grave concerns: Report.

Office of the United Nations High Commissioner for Human Rights. (2024, December 31). Pattern of Israeli attacks on Gaza hospitals raises grave concerns: Report.

Organisation for Economic Co-operation and Development. (2002). Guidelines on the protection of privacy and transborder flows of personal data (OECD Privacy Guidelines) . OECD.

Orkin, M., & Ferraro, T. (2022, July 26). IHL and occupied territory. Humanitarian Law & Policy Blog. International Committee of the Red Cross.

Ottis, R., & Lorents, P. (2011, January). Cyberspace: Definition and implications. In Proceedings of the 5th International Conference on Information Warfare and Security (pp. 267-270). Dayton: Academic Publishing Limited.

Patel, M. (2023, November 4). From hashomer to nili, the history of Israeli intelligence, its successes and failures. The Indian Express.

Peacekeeping and Stability Operations Institute. (2020). Drone case study. U.S. Army War College.

Picus Security. (2024). APT29 Explained: Cozy Bear's Evolution, Techniques, and Notorious Cyber Attacks.

Pietralunga, C. (2024, April 5). Israeli army uses AI to identify tens of thousands of targets in Gaza. Le Monde.

Pun, D. (2017). Rethinking espionage in the modern era. Chicago Journal of International Law, 18(1), 353–382.

Radsan, A. J. (2007). The unresolved equation of espionage and international law. Michigan Journal of International Law, 28(3), 595–624.

Rahman, A. (2024, October 16). Explainer: The role of AI in Israel’s genocidal campaign against Palestinians. Institute for Palestine Studies

Raviv, Y., & Fuchs, A. (2024, April 3). Lavender: The AI machine directing Israel’s bombing spree in Gaza. +972 Magazine.

Raviv, Y., & Fuchs, A. (2024, April 3). Lavender: The AI machine directing Israel’s bombing spree in Gaza. +972 Magazine.

Reuters. (2025, March 6). What is the Five Eyes intelligence-sharing alliance as Trump upends geopolitics?

RFI. (2023, December 16). Funeral held for Al Jazeera journalist killed in Israel strike. RFI.

Rishmawi, M. (2019, November). Protecting the right to life in protracted conflicts: The existence and dignity dimensions of General Comment 36. International Review of the Red Cross, 101(912), 1149–1169.

Rodman, D. (2013). Israel’s silent defender: An inside look at sixty years of Israeli intelligence. Israel Affairs, 19(2), 383–384.

Rommen, R. (2024, April 7). Israel's 'Where's Daddy?' AI system helps target suspected Hamas militants when they're at home with their families, report says. Business Insider.

Schmitt, M. N. (2024, August 13). Total defeat of Hamas: The end of a NIAC? Lieber Institute West Point.

Schofield, D. (2023, December 20). Israeli soldiers are snatching Palestinians' phones and punishing them for having photos of Gaza. Novara Media.

Sebag-Montefiore, H. (2000). Enigma: The Battle for the Code. Weidenfeld & Nicolson.

Sherlock, R., Wood, D., & Bashir, A. B. (2023, November 17). Israel told Palestinians to evacuate to southern Gaza — and stepped up attacks there. NPR.

Shoshan, E. (2015). Applicability of international law on cyber espionage intrusions.

Siegal, T. (2022, December 12). Mossad head reveals how Syria found Eli Cohen, discloses spy’s final message . Times of Israel.

Skinner, C. (2019). ‘Precise’ strikes: Fractured bodies, fractured lives – Israel’s drone wars: An update. Drone Wars UK.

Stead, R. (2019, August 15). Remembering Israel's 'disengagement' from Gaza. Middle East Monitor.

Sterling, B. (2018, November 14). The Paris Call for Trust and Stability in Cyberspace.

Such as Russian spies in the United States or vice versa during and after the Cold War.

Taha, S. (2020). The cyber occupation of Palestine: Suppressing digital activism and shrinking the virtual sphere. Global Campus of Human Rights.

The New Indian Express. (2018, April 8). There are no innocent people in Gaza: Israel defence minister Avigdor Lieberman.

The SOC Labs Team. (2024, July 7). Understanding APT28: A Full Recap of Notorious Cyber Threat. The SOC Labs.

TheSecMaster. (2025, February 18). Double Dragon (APT41). TheSecMaster.

Thomas, G. (1999). Gideon's Spies: The Secret History of the Mossad (pp. 30–43). New York: St. Martin's Press.

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. Journal of Conflict and Security Law, 17(2), 187–209.

Tufekcioglu, H. (2023, February 15). Surveillance of Palestinians and the fight for digital rights. Al-Shabaka.

U.S. Army Field Artillery School. (2024, March 1). Enhancing tactical-level targeting. Line of Departure.

UN General Assembly Resolution 73/98 (2018), A/RES/73/98, 7 December 2018

UN General Assembly Resolution 77/24 (2022), A/RES/77/24, 30 November 2022

UN High Commissioner for Human Rights Bachelet calls Israel's "terrorism" designation an unjustified attack on Palestinian civil society [Press release].

UN Human Rights Committee, Concluding Observations on Israel, CCPR/C/ISR/CO/4 (2014

UN Human Rights Committee, General Comment No. 31, The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13 (2004),

UN Human Rights Committee. (1988, April 8). General comment No. 16: Article 17 (Right to privacy), the right to respect of privacy, family, home and correspondence, and protection of honour and reputation.

UN report: Palestinian detainees held arbitrarily and secretly subjected to torture by Israeli authorities.

UN Security Council Resolution 2334 (2016), S/RES/2334, 23 December 2016

UN Security Council Resolution 242 (1967), S/RES/242, 22 November 1967

UN Security Council Resolution 338 (1973), S/RES/338, 22 October 1973

United Nations General Assembly. (1965). International Convention on the Elimination of All Forms of Racial Discrimination. Treaty Series, vol. 660.

United Nations General Assembly. (1966). International Covenant on Civil and Political Rights. Treaty Series, vol. 999.

United Nations General Assembly. (1990, December 14). Guidelines for the regulation of computerized personal data files (Res. 45/95).

United Nations General Assembly. (2004). Resolution 58/292: Status of the Occupied Palestinian Territory, including East Jerusalem.

United Nations General Assembly. (2021, December 10). Assistance to the Palestinian people (A/RES/76/126).

United Nations General Assembly. (2023, September 5). Report of the Independent International Commission of Inquiry on the Occupied Palestinian Territory, including East Jerusalem, and Israel (A/78/198).

United Nations General Assembly. (2023, September 5). Report of the Independent International Commission of Inquiry on the Occupied Palestinian Territory, including East Jerusalem, and Israel (A/78/198).

United Nations General Assembly. (2024). Resolution A/RES/ES-10/24: Illegality of Israel's presence in the Occupied Palestinian Territory, including East Jerusalem.

United Nations General Assembly. (2024). Resolution A/RES/ES-10/24: Illegality of Israel's presence in the Occupied Palestinian Territory, including East Jerusalem.

United Nations High Commissioner for Human Rights. (2024). Human rights situation in the Occupied Palestinian Territory, including East Jerusalem, and the obligation to ensure accountability and justice (A/HRC/55/28). United Nations Human Rights Council.

United Nations Human Rights Committee. (2004). General comment No. 31: The nature of the general legal obligation imposed on States Parties to the Covenant (CCPR/C/21/Rev.1/Add.13). Office of the United Nations High Commissioner for Human Rights.

United Nations Human Rights Committee. (2014). General Comment No. 35: Article 9 (Liberty and security of person), CCPR/C/GC/35.

United Nations Human Rights Committee. (2018, October 30). General comment No. 36 on article 6 of the International Covenant on Civil and Political Rights, on the right to life (CCPR/C/GC/36).

United Nations Human Rights Committee. (2020). General comment No. 37 (2020) on the right of peaceful assembly (article 21). CCPR/C/GC/37.

United Nations Office for the Coordination of Humanitarian Affairs. (2025, May 9). Verification of damages to schools based on proximity to damaged sites – Gaza, Occupied Palestinian Territory, Update #9. ReliefWeb.

United Nations Office of the High Commissioner for Human Rights. (2024, July 31).

United Nations Office on Drugs and Crime. (n.d.). Cybercrime Module 14: Key Issues – Cyberespionage. Education for Justice.

United Nations Security Council. (2016). Security Council resolution 2334 (2016).

United Nations. (1949). Geneva Convention (III) relative to the Treatment of Prisoners of War, art. 4(A)(2).

United Nations. (1965). International Convention on the Elimination of All Forms of Racial Discrimination. United Nations Treaty Series, vol. 660.

United Nations. (1966). International Covenant on Economic, Social and Cultural Rights. United Nations Treaty Series, vol. 993.

United Nations. (1989). Convention on the Rights of the Child. United Nations Treaty Series, 1577, 3.

United Nations. (1998). Rome Statute of the International Criminal Court.

United Nations. (2005). The Israeli 'Disengagement' Plan: Gaza Still Occupied. United Nations Information System on the Question of Palestine (UNISPAL).

United Nations. (2025, January 3). Security Council debates Israeli attacks on hospitals allegedly misused by Hamas, as UN rights chief urges independent probes (Press Release No. SC/15959).

United Nations. and Diakonia International Humanitarian Law Centre. (2021, November 18). Designation of Palestinian CSOs as “terrorist organisations”. Diakonia.

United States Congress. (1917). Espionage Act of 1917.

United States War Department. General Orders No. 100: Instructions for the Government of Armies of the United States in the Field (Lieber Code), prepared by F. Lieber (1863), art. 88.

Vienna Convention on Diplomatic Relations, arts. 9 & 41(1), Apr. 18, 1961. .

Vilasi, A. C. (2018). The intelligence services in Israel: A short history. Open Journal of Political Science, 7(4), 454–462.

Viveros Álvarez, J. S. (2024, September 4). The risks and inefficacies of AI systems in military targeting support. ICRC Humanitarian Law & Policy Blog.

WACC. (2019, May 13). How Israel controls Palestinian ICTs. WACC Global.

WATERS, B. G. (2016). An International Right To Privacy: Israeli Intelligence Collection In The Occupied Palestinian Territories. CAP. UL REV, 677, 2.

Watkin, K. (2025, February 24). I spy: Espionage, Perfidy, and fighting in the Shadows. Lieber Institute West Point.

Watt, E. (2017). The right to privacy and the future of mass surveillance. The International Journal of Human Rights, 21(7), 773-799.

Weiss, L. (2013). The Lavon Affair: How a false-flag operation led to war and the Israeli bomb. Bulletin of the Atomic Scientists, 69(4), 58–68.

Westfall, S., & Berger, M. (2023, October 26). Family of Al Jazeera Gaza bureau chief killed in airstrike. The Washington Post.

Winkler, J. R. (2009). Information warfare in World War I. The Journal of Military History, 73(3), 845–867.

WIRED., Silva, M. A. (2020). The fundamental conceptual trinity of cyberspace. Contexto Internacional, 42(1), 9–37.

Yoo, C. S. (2015). Cyber espionage or cyberwar?: International law, domestic law, and self-protective measures. Cyberwar: Law and Ethics for Virtual Conflicts (Jens David Ohlin, Kevin Govern, Claire Finkelstein, eds., 2015), U of Penn Law School, Public Law Research Paper, (15-3).

Zalnieriute, M. (2015). An international constitutional moment for data privacy in the times of mass-surveillance. International Journal of Law and Information Technology, 23(2), 99-133.

Zhou, W., & Greipl, A. R. (2024, August 29). Artificial intelligence in military decision-making: Supporting humans, not replacing them. ICRC Humanitarian Law & Policy Blog.

Zhou, W., & Greipl, A. R. (2024, August 29). Artificial intelligence in military decision-making: Supporting humans, not replacing them. ICRC Humanitarian Law & Policy Blog.

Zureik, E. (2016). Strategies of Surveillance: The Israeli Gaze. Jerusalem Quarterly, (66).

الأساليب الإسرائيلية للتجسس الإلكتروني ضد المدنيين في الأرض الفلسطينية المحتلة في ظل القانون الدولي

أحلام أحمد حسن صبح

أعضاء لجنة الاشراف: د. سنيه فيصل حمدي ابو عمرو، د. رائد محمد أبو بدويه، د. يعقوب حلبي

الملخص

تتناول هذه الرسالة دراسة مشروعية أساليب التجسس السيبراني التي تستخدمها إسرائيل ضد المدنيين في الأرض الفلسطينية المحتلة في ضوء أحكام القانون الدولي. فإسرائيل، بوصفها دولة رائدة عالميًا في مجال التقنيات السيبرانية ودولة قائمة بالاحتلال، تستخدم تكنولوجيا متقدمة للغاية لممارسة أنشطة التجسس السيبراني ضد سكان مدنيين يعيشون تحت احتلال عسكري طويل الأمد. وتشمل أدوات التجسس السيبراني الإسرائيلية برامج التجسس مثل «بيغاسوس»، وتقنيات التعرف على الوجوه مثل «بلو وولف» و«ريد وولف»، والمراقبة الواسعة لوسائل التواصل الاجتماعي عبر تقنيات التنميط، والطائرات غير المأهولة لأغراض المراقبة، إضافة إلى أدوات الذكاء الاصطناعي مثل «لافندر»، و«الإنجيل»، و«أين الأب؟». وتثير هذه الممارسات إشكاليات قانونية جسيمة، لا سيما في ظل تصاعد استخدامها بعد 7 تشرين الأول/أكتوبر 2023.

تعتمد الرسالة منهجًا وصفيًا تحليليًا لتقييم مدى مشروعية هذه الممارسات، من خلال دمج أحكام كل من القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان. وتخلص الرسالة إلى أن ممارسات التجسس السيبراني الإسرائيلية في الضفة الغربية تنتهك مجموعة من الحقوق الأساسية المكفولة بموجب القانون الدولي لحقوق الإنسان، بما في ذلك الحق في الخصوصية، وحماية البيانات، والمساواة، والكرامة، والحق في الحياة، كما ترقى إلى مستوى العقاب الجماعي المحظور بموجب القانون الدولي الإنساني. أما في

قطاع غزة، فإن استخدام الأنظمة المدعومة بالذكاء الاصطناعي في تنفيذ عمليات القتل المستهدف يشكل خرقًا للمبادئ الأساسية للقانون الدولي الإنساني، ولا سيما مبادئ التمييز والتناسب والاحتياطات، فضلًا عن انتهاكه للحق في الحياة المكفول بموجب القانون الدولي لحقوق الإنسان.

وعليه، تسهم هذه الرسالة في إثراء الأدبيات القانونية المتزايدة التي تتناول استخدام التقنيات الحديثة في سياقات النزاعات المسلحة، من خلال توصيف أساليب التجسس السيبراني الإسرائيلية بوصفها شكلًا من أشكال القمع الرقمي والاستهداف غير المشروع ضمن سياق الاحتلال.

الكلمات المفتاحية :الأرض الفلسطينية المحتلة؛ التجسّس السيبراني؛ تقنيات المراقبة؛ القانون الدولي الإنساني؛ القانون الدولي لحقوق الإنسان.