2026-01

Ghosts in the machine: How non-state actors like Hamas technologically adapt to level the playing field in asymmetric conflicts

Tsiftsoglou, Vasiliki

þÿœaster in International Relations, Strategy and Security, School of Soci
Humanities, Neapolis University Pafos

SCHOOL OF SOCIAL SCIENCES, ARTS AND HUMANITIES

DEPARTMENT OF HISTORY, POLITICS AND INTERNATIONAL STUDIES

Ghosts in the machine: How non-state actors like Hamas technologically adapt to level the playing field in asymmetric conflicts

Vasiliki Tsiftsoglou

January 2026

SCHOOL OF SOCIAL SCIENCES, ARTS AND HUMANITIES

DEPARTMENT OF HISTORY, POLITICS AND INTERNATIONAL STUDIES

Ghosts in the machine: How non-state actors like Hamas technologically adapt to level the playing field in asymmetric conflicts

This thesis was submitted for distance acquisition of a postgraduate degree in International Relations, Strategy and Security at Neapolis University

Vasiliki Tsiftsoglou

January 2026

Copyrights

RESPONSIBLE STATEMENT

I, Vasiliki Tsiftsoglou, knowing the consequences of plagiarism, I declare responsibly that this paper entitled " Ghosts in the machine: How non-state actors like Hamas technologically adapt to level the playing field in asymmetric conflicts. “, the points where I have used ideas, text and/or sources of other authors are clearly mentioned in the text with the appropriate reference and the relevant reference is included in the section of the bibliographic references with a full description.

The Denotation

Vasiliki Tsiftsoglou

TABLE OF CONTENTS

Student Name: Vasiliki Tsiftsoglou

Postgraduate Thesis Title: Ghosts in the machine: How non-state actors like Hamas technologically adapt to level the playing field in asymmetric conflicts.

This Master's Thesis was prepared during the studies for the distance master's degree at Neapolis University and was approved on 12 February 2026, by the members of the Examination Committee.

Examination Committee:

First Supervisor (Neapolis University Pafos): Marina Eleftheriadou

Member of the Examination Committee: Zakia Aqra

Member of the Examination Committee: Eleni Gavriil

Acknowledgements

To my grandpa.
You were always proud of me until the very end.

This thesis would not have been possible without the guidance and the help of several people who extended their valuable assistance and time in the preparation and completion of this study. I am grateful to the guidance of my supervision, Professor Marina Eleftheriadou, whose guidance and expertise have enabled me to complete my MSc. within the time frame available. I would like to thank Nicolas Oikonomou for encouraging me to take on this challenge when I was unsure of the time and dedication it would require and enduring me throughout the study. It was worth it. A select group of people have been a great source of support while completing my thesis. A large thank you is extended toward Christina Semertzidou, Vasiliki Ntampasi, Sonia Ananiadou, Elsa Kamberi and Thanasis Rizos. They consistently brought a smile to my face throughout the studies and especially this thesis. Lastly, the most significant acknowledgement is reserved for my parents. I am who I am today, also because of them.

Abstract

Non-state actors have increasingly become the primary force in current conflicts, employing unorthodox tactics to battle against state governments. Non-state groups lack sufficient military power to fight against state forces, so they use guerrilla warfare, terrorist attacks and creative military strategies to fight another day while working toward their political goals. Their survival and success depend on ingenuity over brute force, and technology has become their essential operational domain in their effort to gain an advantage over militarily superior state governments. The thesis examined how non-state actors use digital technology in their core activities such as propaganda, radicalization, recruitment of new members, funding, training, and covert operations. The methodology focused on the case study of the Hamas-Israel conflict which provided an excellent opportunity to study how warfare has developed through time and how technology can level the playing field between non-state and state actors. Hamas has used technology innovatively to counter Israel's superior conventional military power. The thesis studied how the group evolved through its history from basic community-based training with simple rockets into its current hybrid operation which led to the October 7 attacks. The study observed that the operation combined various low and high-tech innovations to achieve a destructive outcome which proved that creative tactical approaches can take advantage of defense systems that depend too heavily on advanced technology. In the aftermath of the attack, the Israeli government has accelerated its technological progress through the deployment of AI-based targeting systems, autonomous drones and its extensive monitoring of Gaza. That shift underscores a core dilemma: whether the most advanced technological systems can resolve the strategic and human intelligence deficits which asymmetric threats have exposed or if they will create more efficient yet vulnerable systems. The Israel-Hamas conflict seems to have defined a new era of warfare, where innovation and adaptation may be the ultimate weapons.

Keywords: Asymmetric warfare, Non-state actors, Technological adaptation, Hamas, Cyberspace, Social media, Propaganda, Radicalization, Recruitment, Encrypted messaging, Cryptocurrency, Commercial drones, Low-tech tactics, Tunnels, Iron Dome, Over-reliance, AI warfare, Autonomous systems, Lavender (AI targeting), Facial recognition, Mass surveillance, Arms race, Ethical challenges, HUMINT, OSINT.

Chapter 1 - Introduction

The conventional military image of war, which shows countries fighting each other on established combat zones, is fading. In the 21st century, non-state actors now increasingly influence the nature of conflicts. These organizations consist, amongst others, of insurgent groups, liberation movements and terrorist organizations which function outside state authority and aim to gain power through unofficial means. Their ability to perform unconventional warfare makes them more powerful than using conventional military tactics. Non-state groups use guerrilla warfare together with terrorist attacks and their ability to create new strategic approaches to fight against stronger state enemies who seek to eliminate them. The strategic domain of technology functions as an essential base which non-state groups need. Digital tools provide them with accessible, low-cost, and anonymous channels to bypass state controls. They enable every core function of modern asymmetric conflict: propaganda, radicalization, recruitment, financing, planning, and intelligence.

This dynamic creates the main research question of this study, which focuses on:

- How non-state actors use technology in innovative ways to fight against state adversaries and level the playing field?

The non-state group Hamas functions as an excellent research subject as it demonstrates how non-state actors can use creative asymmetric methods to fight against stronger state forces. The group used digital tools alongside conventional methods which included drone technology and AI-generated propaganda as well their sophisticated network of underground tunnels to show how modern technology can shrink the gap against more superior military capabilities. In response, the Israeli military launched a war effort at an accelerated pace following the attacks which relied heavily on surveillance data and AI to create targets and control attacks.

Thus, the inquiry is explored through two sub-questions:

- How has Hamas used technology to fight against Israel's superior conventional military power?
- What has been the nature of Israel's technological response to Hamas's asymmetric tactics, after October 7, 2023?

The Hamas-Israel conflict is the key research case of this thesis. It shows a clear trajectory of Hamas's low-tech beginnings to a sophisticated, integrated model of hybrid warfare. The October 7 attacks were the result of Hamas's long-term deliberate technological development and adaptation; It started with basic rocket attacks and progressed to cyber espionage, drone swarms and encrypted application usage that successfully took advantage of weaknesses in the Israeli sophisticated military system.

In the war that followed the attacks, it became evident that the current conflict functions as a testing ground for military technology, including advanced targeting systems that will define the nature of future warfare. The Israeli government has speeded up its modernization process through AI-based targeting systems and drone technology and extensive surveillance operations in Gaza. The situation creates a core dichotomy as new technology systems while seemingly possessing the ability to address human and strategic intelligence weaknesses they may create more vulnerable operational systems and a larger attack surface.

1.1 Why this research matters

The answer to these questions holds value because it highlights three connected factors which impact worldwide security systems. First, it provides essential empirical research regarding an active military conflict demonstrating how modern warfare technology functions through actual battlefield observations. The October 7 attack created a strategic shock because it proved that all security systems built through modern physical and digital security funding during the last few decades would not protect against attackers who used basic innovative methods with specific digital instruments. The current situation functions as an instant model which other non-state organizations across different areas can use and learn from. Second, the research shows a potentially dangerous feedback loop which can accelerate at an increasing rate in future conflicts. The development and deployment of inexpensive commercial technology by non-state actors can force states to implement more sophisticated and costly systems leading potentially to an arms race. It also raises key ethical and legal issues about the role of human judgement in warfare, whether compliance of AI-controlled attacks comply with the rules of engagement, as well as the impact of continuous digital surveillance. Finally, the implications of this research extend far beyond military doctrine to the very structure of international security. The ability of non-state

actors to use technology for asymmetric operations against strong states creates a challenge to conventional deterrence systems which can result in changes to worldwide power dynamics.

1.2 Methodology

The thesis makes use of qualitative methodologies to develop an understanding of a complex and developing security phenomenon. The research employs a comparative perspective within a single case study focusing on the technological dimensions of the conflict between Hamas and Israel. It is based on a systematic review and synthesis of diverse sources including academic studies, official government documents, security think tank papers and investigative reports from leading international news outlets. The comparative analysis follows a thematic organization as it investigates how different actors use technology across parallel domains. These include propaganda and information warfare, intelligence and cyber operations as well as training and weapons systems. This methodology allows for the exploration of not just what technologies are used between non-state and state actors, but also how and why they are adopted in response to the adversary's capabilities. In this way, the methodology provides a structured lens to answer the research questions about adaptation, response, and the resulting implications for the character of future warfare.

Chapter 2 - Understanding non-state actors

The image of war as a clash between national armies on a defined battlefield seems to be becoming a relic of the past. Modern conflicts have shifted away from the traditional battles between national military forces. The 21st century has seen the increasing involvement of non-state actors that use unorthodox methods to fight against established authorities in asymmetric conflicts. Simply put, a non-state actor refers to a political or military person or group that does not possess national status but does wield significant influence (Gentry 2016, 470). It is, however, important to distinguish between violent non-state actors (VNAs) and non-violent non-state actors (NVNAs). VNAs include insurgent groups and terrorist net works that are not controlled by governments control and use military or terrorist attacks to achieve their objectives for autonomy and political power (Gentry 2016, 472). Examples include Al Qaeda and Colombia's FARC. On the other

hand, NVNAs avoid violence and instead focus on indirect influence through political advocacy, networks, and information campaigns (Gentry 2016, 470). The military strength gap between powerful and weak forces leads to asymmetric warfare as their fighting abilities and available resources differ greatly. The weaker side employs tactics such as guerrilla warfare and terrorism, to target the weaknesses of their stronger opponents since they lack the ability to fight conventionally (Paul 2007, 203).

2.1 How non-state actors operate; common aims and constraints

Non-state actors who engage in asymmetric conflict develop their strategic plans through attacks on four linked objectives (Cronin 2006, 86; Al Raffie 2025, 5). First, a non-state group needs to protect its existence from state attempts to eliminate it. To achieve this, it develops asymmetrical tactics and can also seek outside help to maintain its operational activities. Second, non-state groups also seek political validation because they must prove that they're the authorized representatives of their people and their movement. The process of acquiring territorial control operates alongside political legitimacy campaigns which focus on specific geographic areas. The last strategic objective of these actions consists of establishing state instability through ongoing attacks against government and law enforcement institutions.

Non-state actors experience ongoing external security threats and potential internal instability. The main force which affects their operations consists of advanced state military capabilities that continue to evolve. Governments can use modern intelligence collection techniques along with financial restrictions from banking sanctions and asset freezing to block non-state groups from accessing international banking systems (Johnston et al. 2023, 3; Kurtulus 2012, 50). This external pressure includes nowadays also private military companies which states use to conduct their counterterrorism and counterinsurgency operations. For example, the Wagner Group provide private counterterrorism (CT) and counterinsurgency (COIN) services which perform destructive military operations to reshape security patterns in affected areas while providing patron states with plausible deniability, to an extent (Felbab-Brown 2023).

Non-state groups have limited resources and are usually being watched by advanced government systems. They need to use clever tricks and flexible tactics instead of traditional military ones to survive and their success relies on their creativity and

dedication (Beccaro 2022, 798; Cronin 2006, 86). To begin with, non-state groups distribute propaganda and employ strategic communication tactics to gain public support from local populations as well as foreign backing. Furthermore, non-state actors need to evolve into adaptable distributed networks to navigate effectively the constraints they face (Gentry 2016, 474). This transformation to networked organizations makes them more able to resist countermeasures, and also more difficult to predict in their operations, which creates major difficulties for conventional security systems. This transformation also extends to adapting to small-scale modular military operations and surprise guerrilla attacks, with limited funding received many times through illegal activities and financial systems that operate within expatriate communities (Johnston et al. 2023, 15).

Such restrictions fuel innovative solutions, leading to the creation of a hybrid model of operations. This model combines physical activities with digital resources to help non-state groups develop evasive tactics to outmaneuver states and avoid direct confrontation with them (Winter et al. 2020, 5). The battle to continuously "adapt to survive" nowadays takes place heavily in cyberspace, where non-state actors leverage technological innovation, in creative ways to level an asymmetric playing field in their struggle against states.

2.2 How cyberspace enables non-state actors

Non-state actors use cyberspace as their strategic domain to create their own power rules and influence operations. Its ease of access and low cost of entry enable non-state organizations to connect en-mass with audiences spanning generations and demographics. The rich digital environment allows propaganda makers to tailor specific content for different platforms and audiences through a wide range of multimedia channels, from magazines such as AQAP's "Inspire" magazine, to encrypted messaging services. On top of that, digital operations can maintain speed and anonymity, which makes it more difficult for states to identify sources and respond effectively. Furthermore, digital presence also demonstrates high resilience, as banned websites can be easily restored through quick server transfers and new domain names. For example, a Salafist jihadi website can start operating again through server relocation to a new domain which maintains full content accessibility within a brief timeframe (Beccaro 2022, 790). This way, non-state actors can create their own content and control their narrative since this digital environment enables them to avoid media monitoring systems and bypass traditional mainstream media gate

holders. (Mair 2020, 25). This becomes even more relevant as state pressure in the digital space has increased with governments working together with major technology platforms to implement control measures and cut off essential communication paths which non-state groups depend on for propaganda and fundraising activities (Frenkel & Hubbard 2019).

Nowadays, non-state actors use cyberspace as a critical space of operations, which enables them to perform essential activities from propaganda distribution and recruitment to financing without always requiring physical locations. Non-state actors also use digital platforms to perform more complex operations such as training of their members in online classrooms, as well as weapon and material procurement from encrypted marketplaces and advanced intelligence collection through cyber espionage and OSINT methods. The digital environment is not just a supporting tool anymore. It operates as an independent domain which enhances physical capabilities, thus changing the face of asymmetric warfare forever.

2.2.1 Recruitment and radicalization

Non-state actors successfully use cyberspace to carry out their recruitment and radicalization efforts (Drăgan 2024, 256). The conversion of online curiosity into physical participation follows a structured sequence which includes three distinct stages. Groups start their recruitment process by sharing appealing propaganda materials with potential new members. The organization creates trust-based relationships through social networks which exist in digital and physical environments to develop membership feelings among its members. Finally, the organization requires potential recruits to execute actions which also extend past virtual space (Winter et al. 2020, 8). This structured process, however, depends on first cultivating the ideological conditions that make an individual receptive to recruitment in the first place.

The process of radicalization develops slowly when people discover beliefs which lead them to adopt an "us-versus-them" perspective and stronger feelings of belonging. Radicalization today often starts with a simple scroll with the internet providing easy access to such content. The combination of online echo chambers with algorithm-based systems enables radical views to spread while preventing balanced discussions. This creates an environment where dangerous theories and hateful content can flourish. The

malicious algorithms operating on these platforms facilitate the conversion of curious and impressionable users to dedicated ones, especially amongst digital natives who spend most of their time online. For example, for the tech-savvy generations like Gen Z and Gen Alpha, such extremist content social media platforms can be both familiar and interesting. Research shows that TikTok influencers have used fast-paced social media content to spread extremist messages which has grown the number of digital recruits for ISIS (Stockhammer 2025, 16). It also seems that different technologies enhance radicalization through distinct mechanisms. Social media platforms including TikTok, YouTube and 4Chan and Reddit create environments for extremist speech to develop while Telegram and Rocket.Chat provide secure encrypted channels for further radicalization and commitment as they also offer users feelings of protection and privacy (Stockhammer 2025, 20).

Radicalization does not happen by itself but exists as an actively developed process. This dangerous transformation is linked to advanced propaganda efforts made by non-state groups which aim to speak directly to the minds and souls of the impressionable using narrative techniques to create an attractive alternative worldview that fuels the very radicalization process.

2.2.2 Messaging and propaganda

Non-state actors leverage cyberspace to craft and distribute propaganda, aiming to directly shape public opinion through mass communication. The main distribution platforms for premeditated content include social media platforms, websites, and blogs with the frequent use of professional editing to maximize its impact. The digital presence of non-state groups allows them to share their complaints and showcase their military activities while keeping a degree of safe distance. For example, the Westgate Mall attack in Nairobi became a real-time information warfare operation when the non-state group Al-Shabaab used Twitter to distribute tactical updates (Mair 2020, 25). The digital presence of non-state groups continues to evolve instead of disappearing when faced with government and corporate efforts to suspend their social media accounts. For example, Hezbollah despite its social media accounts suspension, it still maintains its outreach activities by migrating to alternative platforms and through supporter networks and proxy operations which continue

to distribute propaganda to mobilize both sympathy and funds (Frenkel and Hubbard 2019).

It may sound like something that belongs to the corporate world, but non-state actors also depend on building a trustworthy brand. This helps them draw in financial support, necessary to fund their operations. The process runs as a self-reinforcing cycle: Better brand awareness links to increased donation levels that support the development of better content and messaging that boosts the brand's worth and attracts more support. Non-state actors build their brand identity through digital platform growth and develop powerful online content which shows their organization as strong and resilient. For example, Hamas uses branding methods which match those of international businesses (Mozes and Weimann 2010, 1) while the Afghan Taliban operate a "virtual emirate" to manage their image and influence (Wege 2016, 836). Finally, online publications like AQAP's "Inspire" and the Islamic State's "Rumiyah" presented operational instructions together with ideological justification, which not only provided functional advice but also built the organization's strategic communications (Reed and Ingram 2017, 5).

Emerging technologies, which include artificial intelligence (AI) and deepfakes, are adding a new layer to the propaganda of non-state groups. For example, the extremist network "NazTok" actively uses AI to bypass automatic platform moderation (Alexe 2025). AI technology can also facilitate emotional manipulation as it allows non-state actors to generate deceptive content through speech cloning, such as the cloned speeches of Adolf Hitler. This alters historical facts and weakens moral opposition, making impressionable users more susceptible to radicalization (Alexe 2025). Furthermore, deepfake technology enables the creation of fake images which can make non-state organizations seem more appealing to new members. For example, the Islamic State and other terrorist groups use deepfake technology to create deceptive visual content which presents terrorist life as glamorous while creating false religious reasons for violence and using humorous material to build group unity (Busch and Ware 2023, 7). Non-state groups employ these tools to generate customized propaganda which evades detection while establishing deep emotional connections with viewers, speeding up the radicalization process.

2.2.3 Cyber espionage and intelligence operations

Propaganda and recruitment don't just spread ideologies. They also enable intelligence operations. Non-state actors implement Open-Source Intelligence (OSINT) in their operations because it provides them with affordable data collection and adversary monitoring capabilities which enables planning support without requiring expensive spy networks (Flamer 2023, 1171) OSINT requires organizations to analyze publicly accessible data which results in useful intelligence reports. It serves as the main data collection tool for non-state actors because it delivers vital information at budget-friendly costs (Gentry 2016, 483). The groups obtain their data mainly from monitoring social media platforms and news outlets, and through analyzing states' policy in order to determine their operational capabilities and target preferences. Furthermore, non-state groups can make use of open academic research and public databases to assess public opinions which they apply for creating their strategic plans.

The use of OSINT enables non-state actors to operate without requiring expensive spy networks because it provides them with advanced intelligence capabilities. For example, Hamas uses OSINT to study Israeli military operations and civilian activities which helps them develop their strategic plans (Flamer 2023, 1174, 1182). Beyond information gathering, non-state actors also use OSINT data to perform cyber operations for espionage purposes by integrating publicly available data with decision-making processes (Gentry, 2016, 474; Al Raffie 2025, 18). Multiple organizations show this operational pattern through their separate operational activities. For instance, Hezbollah operates an adaptable cyber espionage system which utilizes open data sources and ISIS uses budget-friendly cyber capabilities to operate drones for reconnaissance and attack missions which help them achieve military expansion (Beccaro 2023, 794).

2.2.4 Operational planning and use of messaging platforms

The evolution of non-state actors into networked organizations makes them more difficult to detect and predict which creates substantial problems for established security systems. Their operational transformation is built upon standard messaging applications and online forums which can serve as their core operational center (Winter et al. 2020, 7). In this setup, leaders use unofficial communication channels to give strategic orders to frontline units who subsequently manage their missions through various websites and platforms

(Cronin 2006, 85). Remote coordinators direct operatives in target countries through what's called "virtual planning" for mission preparation. It includes target identification, teaching attack methods, as well as ideological and logistical support. The Islamic State used virtual planning as its main method for external operations which resulted in 16 out of 38 European terror plots between January 2014 and October 2016 receiving some form of online instructions from the group's networks (Dass 2024). The digital tools used in operational planning maintain essential internet connectivity which create immediate feedback channels between planners and field operatives even when state actors block official communication paths (Winter et al. 2020, 6).

2.2.5 Financing

Non-state actors operating in cyberspace distribute their funding across multiple channels instead of depending on one method to support their activities. These actors maintain their funding networks through public platforms, encrypted channels, and proxy media ecosystems which operate between international borders. The system protects user anonymity while performing financial operations through multiple nodes, which stay operational even when one node fails (Handler 2022). Groups employ diaspora networks together with proxy media platforms to operate when their direct funding channels become inaccessible. Militant networks operate through proxy platforms because these platforms let them keep their financial systems and communication channels active after major platforms banned them (Frenkel & Hubbard 2019). For example, the social media campaigns of al-Qaeda and IS have enabled their volunteer supporters to raise millions of dollars through fundraising efforts (Winter et al. 2020, 9). Non-state actors also receive financial support through digital criminal activities which include cryptocurrency operations and ransomware attacks and other cyber-based schemes. For example, ISIS operated by selling weapons and drugs and through human trafficking before converting the funds into cryptocurrency (Handler 2022).

2.2.6 Education and training

Non-state actors are not confined anymore to their traditional training camps, as they can now perform their essential training operations via online platforms. The case of the Tsarnaev brothers who received bomb-making instructions from Al Qaeda's Inspire magazine and were radicalized mainly online shows how digital encouragement can

quickly turn into dangerous real-world situations (Cooper, Schmidt and Schmitt 2013). The training process starts with propaganda campaigns that contain entertaining yet educational content. For instance, Hamas's children's online magazine Al-Fateh combined militant ideology with children’s stories (Levitt 2007, 2). From there, the training process advances to be more direct and sophisticated. For example, the Islamic State Khorasan Province (ISKP) uses encrypted platforms to deliver multi-week online training programs and teach general digital skills as well as advanced AI techniques with the aim of developing online propagandists and technical experts (Firdous 2024). ISKP also provides its members with full technical documentation, which explains how to convert standard drones into autonomous systems (Dass and Basit 2025). The training program ends with remote individualized guidance and mentorship sessions. For instance, Telegram allows experienced operatives to conduct virtual mission briefings and encrypted "cyber coaching" sessions for psychological support (Stockhammer 2025, 17).

Furthermore, non-state groups also use customized game modifications of popular video games such as Grand Theft Auto and Call of Duty to teach violence normalization and tactical simulations, which turn entertainment into operational training (Ogele 2024, 31). The RAND Corporation analyzed Al-Qaeda activities in modifying video games through their "ISIS: The Video Game" and "Mujahideen" Counter-Strike mods, which functioned as training tools and recruitment platforms (Ogele 2024, 34). It seems that non-state groups make use of all types of content, from children's magazines to drone manuals and video games, to establish a protected digital ecosystem for member training.

2.2.7 Weapons and the dark web

Technology is also enabling non-state actors to arm themselves, bypassing sealed borders and a lack of foreign allies. (Wesdorp 2023). Non-state groups tend to procure their required items through digital black markets as these platforms provide the necessary anonymity. The dark web operates as an untraceable marketplace which enables non-state groups to obtain firearms and ammunition and learn how to use them. Users of the Silk Road and AlphaBay platforms can access the "Terrorist's Handbook" together with fake documents and dual-use chemicals which could assist in biological weapon development (Awasthi 2024, 7). The dark web also allows non-state actors to obtain blueprints and

materials and illegal goods which they use to create 3D printed weapons while avoiding standard weapons control laws.

For instance, the Myanmar rebels face well-equipped military forces by using 3D printing as a key weapon production method despite its limited effectiveness. The first FGC-9 rifle was printed during the 2021 coup's beginning and needed only two weeks and $500 to manufacture (Ortiz 2023). The plastic guns made through 3D printing lack durability, but rebels use them for defensive operations and quick attacks to obtain better weapons from the Tatmadaw, Myanmar’s army forces (Eydoux 2022). The printed weapons function as affordable weapons which enable rebels to obtain better conventional arms for frontline combat (Primitivi 2024). In recent years, right-wing extremists have also used 3D printing to produce firearms for attacks. For example in 2024 there were planned attacks on an Islamic education center in Leeds UK, using 3D-printed FGC-9 rifles (Dass 2025). In Portugal, a far-right extremist cell was found in a possession of several 3D-printed firearms, during a raid in June 2025 (Dass, 2025). Finally, the most notable example is that of Stephan Balliet in Germany who used several homemade weapons, included 3D-printed firearms in his attempt to attack a synagogue in 2019 (Listek 2024).

Chapter 3 - Four decades of conflict: The Hamas-Israeli struggle until October 7

The conflict between Hamas and Israel has evolved through different stages of political and military battles as well as ongoing security emergencies that have forever transformed the security landscape of the Middle East. From Hamas's founding during the First Intifada, the violent opposition to the Oslo peace process, the seizure of Gaza and the cycles of devastating war that followed, have all led up to the unprecedented attack of October 7, 2023. The conflict established a permanent state of regional instability which continues to generate security challenges that affect the region to this present day. This part looks at the events and conflicts between Hamas and Israel from the rise of Hamas to October 7, 2023, in order to understand how they affect current discussions on peace and security.

3.1 The rise of Hamas and early confrontations

Hamas was founded in 1987 during the First Intifada, emerging from the Muslim Brotherhood (Drăgan 2024, 241). The group combined the Brotherhood's religious and social organization with an organized military arm (Ranstorp 2025, 17). In the late 1980's Israel reportedly tolerated and even allowed Islamist organizations to expand to counterbalance the more secular PLO (Ranstorp 2025, 16). The 1988 Hamas Charter created a religious and nationalist framework for the conflict, it didn't recognize the state of Israel and completely rejected all negotiations with it (Drăgan 2024, 242), It also rejected the idea of a two-state solution (Ranstorp 2025, 16). However, in the revised Charter of 2017, Hamas pivots from their original positions, implicitly recognizing Israel and stating that there is no religious conflict against the Jewish people but one solely against the "Zionist project" (Hroub 2017, 102). Hamas used the first Intifada to build its influence through popular protests which established its position as a militant organization apart from the Palestine Liberation Organization (PLO) (Margolin 2020, 1078).
The signing of the Oslo Accords in 1993 was a crucial historical event with Hamas members and far-right movements in Israel viewing the Accords as a betrayal. Hamas launched suicide bombings throughout the 1990s to fight against the peace process which it strongly opposed (Chen 2012, 113). Furthermore, the massacre of Palestinians in Hebron in 1994 by the Israeli settler Baruch Goldstein, prompted more violence and undermined further the fragile Oslo peace process. A wave of bombings followed which intensified the public outrage in Israel, strengthened Israel's right wing, despite the ban of the Kach movement and eroded the hope for a peaceful coexistence. The assassination of the Israeli Prime Minister Yitzhak Rabin in 1995, by an Israeli extremist, sealed the fate of the failing peace process. At the same time, the Palestinian population was losing all trust in the Palestinian Authority's ability to deliver results which made Hamas more popular (Ranstorp 2025, 19).

The Second Intifada (2000-2005) broke out after years of Palestinians being frustrated with a peace process that brought neither peace nor sovereignty. Its trigger was Ariel Sharon's - the then leader of the Israeli opposition - high-profile visit to the Mount Temple/ Haram al-Sharif, escorted by hundreds of Israeli forces, which was considered a major provocation amongst the Palestinians (Ranstorp 2025, 19). It quickly developed into a major conflict with clashes both in the West Bank and in Gaza with Hamas conducting military operations and an increasing number of suicide bombings (Chen 2012, 112). The Israeli military launched multiple large-scale operations, targeted assassination and established strict blockades and checkpoints to combat Hamas (Chen 2012, 113; Freilich 2015, 366). The Israeli military strikes against Hamas resulted in substantial Palestinian civilian deaths which further complicated future peace negotiations between the two sides (Freilich 2015, 366).

The Israeli withdrawal from Gaza in 2005 created a pivotal moment which transformed the conflict. The then prime minister Ariel Sharon led the withdrawal of Israeli residents and security forces from Gaza, a unilateral decision stemming from the Israeli frustration with the heavy and never-ending casualties and Israel's inability to stop the violence (Freilich 2015, 362). The withdrawal of Israeli forces from the Gaza Strip created an opportunity for Hamas to seize control and fill in the power vacuum that was left behind. Hamas won the 2006 Palestinian legislative elections and then defeated Fatah in a civil war to establish complete military control of the Gaza Strip in 2007, forcing Fatah forces and officials to leave (Barnea 2024, 1061). The Israeli withdrawal from Gaza resulted in Hamas becoming more powerful and established permanent divisions between Hamas in Gaza and Fatah in the West Bank (Barnea 2024, 1061). Finally, after Hamas seized control, Israel and Egypt enforced complete blockade which devastated the economy of the Gaza Strip, while creating a deep humanitarian emergency. In response to that, Hamas and other factions continued to launch rockets at southern Israel which resulted in civilian deaths and widespread public terror (Ranstorp 2025, 20).

3.2 Major wars between Israel and Hamas

There have been four major military conflicts between Israel and Hamas, since Hamas took control of the Gaza Strip in 2007 until the October 7 attacks. The Israeli military launched Operation Cast Lead in 2008 as response to Hamas's rocket attacks against

Israeli territory and with the goal to weaken Hamas (Barnea 2024, 1061). The military operation against Hamas resulted in major damage to their military bases and underground tunnels and caused significant harm to Palestinian non-combatants (Barnea 2024, 1061, 1062).

The Israeli military launched Operation Pillar of Defense in November 2012 by killing Ahmed Jabari who served as Hamas military commander followed by 1500 Israeli airstrikes against Gaza targets (Barnea 2024, 1063). Hamas launched 1506 rockets during the one-week conflict which included attacks on Tel Aviv and Jerusalem while Israel's Iron Dome system intercepted 421 projectiles which led to decreased rocket attacks in the following year (Barnea 2024, 1063). The conflict demonstrated that military technology had achieved a higher level of sophistication during that time. Namely, the Israeli military used Iron Dome missile defense systems to stop a significant number of rockets which protected Israeli citizens while changing the course of the conflict (Barnea 2024, 1063). The third major conflict was the Operation Protective Edge. It became the longest conflict before 2023 when Israel launched it on July 8, 2014, to respond to the kidnapping and murder of three Israeli teenagers. The conflict resulted in more than 10000 casualties on both sides and 2000 Palestinian deaths. During the conflict there was a barrage of rockets from Hamas whilst Israel focused on destroying the tunnel network, rocket launchers and ammunition deposits (Barnea 2024, 1063, 1064).

Finally, the 2021 Operation Guardian of the Walls was launched by Israel, when Hamas and Palestinian Islamic Jihad launched over 4000 rockets at Israel also targeting Jerusalem, following weeks of clashes and tensions in Jerusalem. Israeli intelligence was initially caught off guard; Israeli forces conducted airstrikes on the Gaza Strip which caused substantial damage and loss of life (Barnea 2024, 1064). The intelligence failures which occurred before the conflict made Israel underestimate Hamas's willingness to escalate, with Israeli Intelligence agencies basing their analysis on incorrect beliefs about Hamas military capabilities and decision making (Barnea 2024, 1064).

3.3 The road to October 7

Hamas built up its military strength through expanded tunnel networks, drones, hexacopters and enhanced rocket capabilities, before launching the October 7 attacks (Ranstorp 2025, 22). Furthermore, despite ongoing Israeli and Egyptian blockades

(Ranstorp 2025, 20), the group ran clandestine military operations to acquire weapons and rebuild its arsenal also by exploiting Israeli intelligence weaknesses and communication breakdowns. The Israeli intelligence gaps were made worse due to insufficient inter-agency cooperation and a persistent underestimation of Hamas's preparations and willingness to initiate a large-scale offensive (Ranstorp 2025, 22). This buildup led to an extraordinary attack that destroyed fundamental ideas of Israeli security and revealed systemic weaknesses that were much larger than just one intelligence failure. In response, Israel launched a large-scale military invasion of the Gaza Strip accompanied by airstrikes, a tightened blockade and a wider conflict against Iran-backed organizations in the region. The ongoing conflict has transformed global security, showing that even technologically advanced defense systems are susceptible and can be overcome by strategic surprise and tactical creative attacks.

Chapter 4 - How Hamas has used technology to level the playing field

For many years, the armed struggle between Israel and Hamas has been marked by an imbalance in military power. On one side, there is a nation-state with one of the most technologically advanced militaries in the world. On the other side, there is a non-state group that started off with basic weapons and recruitment methods. Nevertheless, throughout its history Hamas has leveraged ongoing technological innovations to offset Israeli military's superiority, reaching its peak in the attacks on October 7, 2023 (Levy 2024, 5).

Hamas's innovation efforts go back to the analog days. The Izz al-Din al-Qassam Brigades, its military branch, was created in the early 1990s and at first focused on easily accessible arms such as AK-47s and improvised explosive devices (Groppi and da Cruz Amador 2023). The Qassam rocket was an important early development since it let Hamas attack targets outside of Gaza, even if it wasn't very precise since it lacked a long-range capability (van Coller 2024, 3). Furthermore, Hamas also strategically employed tunnel warfare by building underground networks that supported military operations, troops, and logistics (Levy, 2024, 4). These were low-tech solutions for high-tech problems intended to get beyond Israel's border and air control of the Gaza strip.

It was the digital era that made it possible for the real transformation to take place. Hamas increased their spending in technology after realizing that the internet could magnify the group's reach. By using social media platforms to fulfill its recruitment and propaganda goals, the group was able to spread its message to sympathizers all over the world, who then could potentially turn into hardline followers, in a shorter timeframe. Furthermore, by the late 2010s, Hamas had advanced its cyber espionage capabilities into highly sophisticated operations. In one prominent 2018 campaign, its operatives developed malware Android apps to infect Israeli soldiers' phones, including a malicious application for World Cup scores (Groppi and da Cruz Amador 2023). In addition to getting access to the camera and microphone functionalities and obtaining sensitive military data, the programs employed malware to also obtain user location data (Groppi and da Cruz Amador 2023).

The battlefield also witnessed innovation when the Hamas's fighters developed effective combat strategies, using ordinary gear, that worked against highly advanced military infrastructure. Hamas did a lot of research on Israeli defense technologies, such as the Iron Dome missile defense system and the so-called "Iron Wall" along the border with Gaza. The group discovered that when organizations rely on technology excessively, it can potentially create vulnerabilities (Carchidi 2023). During the October 7 attacks, Hamas used commercially accessible drones to drop bombs on communication towers and weapon warehouses along the border, which blinded the Israeli Defense Forces (IDF), at first. Then, to offer cover to the ground attack, Hamas unleashed an unparalleled barrage of thousands of rockets in only a few minutes, testing the saturation point of the Iron Dome (Carchidi 2023). Finally, the attackers were able to get through circumventing the security fences by using modified drones, explosives, and paragliders as the Israeli sensors were unable to detect objects that flew slowly (Carchidi 2023).

Perhaps most critically, Hamas weaponized Israel's own technological mindset. The Israeli Defense Forces (IDF) seem to depend extensively on automated surveillance and AI-targeting systems which had potentially created an inflated sense of security and made the military less vigilant near the Gaza border (Carchidi 2023). The planning of the attack was shockingly analog: avoiding digital communications that could be intercepted and using the physical cover of routine border protests to conduct reconnaissance. The outcome of the October 7 attacks revealed how basic creative thinking which deeply understands

enemy reliance on advanced technology systems can produce unexpected and catastrophic attacks.

Today, Hamas continues to evolve despite the major blow it got during the prolonged conflict. Its supporters seem to be exploring next-generation tools, such as AI-based propaganda and deep fakes (Nelu 2024). Even though the group's military performance has declined, its path demonstrates that seemingly weak military forces can create new unorthodox ways to fight another day and that technological innovation is not the sole domain of the powerful.

4.1 Radicalization and recruitment

Hamas's radicalization campaign started with one-on-one indoctrination before it turned into a more intricate digital ecosystem. The group used a deliberate approach to build a certain ideological framework that starts in childhood and builds a culture ready for mobilization. For example, Hamas relied on its "Dawa" program, which functioned as a social-welfare network including charities, schools, mosques, and summer camps (Levitt 2007, 1; Ranstorp 2025, 17). The program provided important services to the most disadvantaged individuals with the goal of also building dependence and good will before asking for support. Furthermore, through its regular activities, Hamas established a strong presence in the Palestinian community and became an integral part of people' daily lives. For example, there have been ceremonies at kindergartens run by Hamas featured kids holding toy guns while dressed in military uniforms (IICC 2007,4; Levitt 2007, 3). The indoctrination program started moving online when Al-Fateh, a weekly online magazine for kids, launched in the early 2000s. The website used cartoons with articles that encouraged violent behavior and a fighting spirit (Levitt 2007, 4). Furthermore, summer camps that grew to accommodate thousands of young people provided leisure activities alongside military-style training and an educational curriculum (Choi 2016;Levitt 2007, 3). The universities were also key locations for recruitment because Hamas-controlled student groups, like the "Islamic Bloc", had a strong presence and spread propaganda around campus to attract students and build a loyal base of Hamas' supporters (Levitt 2007, 3; Ranstorp 2025, 17).

Furthermore, the internet has enabled Hamas and its supporters to run virtual recruitment operations. For example, the organization has recruiters who work virtually through social

media platforms to discover new members before moving them to encrypted apps for secure money transfers and operational planning. This model, which is probably inspired by the Hezbollah's "virtual entrepreneurs" recruitment model, enables Hamas to have a wider reach in affordable ways that also maintain operational security (Shkolnik and Corbeil 2019, 28). For instance, the group adopted encrypted messaging apps like Telegram as its key online messaging system. The three major social media platforms X (formerly Twitter) Facebook and YouTube have blocked the group's content but Telegram established itself as an unshakeable platform (Thompson and Isaac 2023). Telegram serves as the tool for building online communities with very limited content moderation, and the combination of graphic content with emojis creates an emotional response in viewers which can lead to violence desensitization and validation through peer-approval.

Finally, the core element which is the catalyst of Hamas' radicalization and recruitment efforts is propaganda. From low-tech mosque posters to Telegram videos Hamas aims to shape the perceptions inside the Gaza strip and beyond. The group's propaganda speaks directly to the grievances and aspirations woven into daily Palestinian life, ensuring that radicalization is not a passive outcome but the goal of an active strategy to reshape public perception and maintain its struggle against Israel.

4.2 Propaganda

The propaganda operations of Hamas have developed into a complete digital information warfare system which uses multiple platforms for its operations. The October 7 attacks represented the most devastating expression of this transformation. It showed how the group has evolved in using technology over time, moving from community building work to conducting real-time information campaigns that affected worldwide public opinion and surprised their enemy. The foundations of Hamas's influence were established through low-tech, community-based methods long before the advent of digital media, which involved face-to-face contact, mosque sermons and audio recordings of speeches which Hamas distributed through cassette tapes and printed pamphlets (Zelkovitz and Limor 2025, 296).

The rise of satellite television and internet access allowed Hamas to create its first successful modern mass media operations, starting for example its own TV channel, Al-Aqsa TV, and reaching viewers directly. It also ran multilingual websites, such as the

Palestine Information Center (PIC), as the main place to get political and operational information (Zelkovitz and Limor 2025). The group also set up official and unofficial English-language profiles on YouTube, Facebook, and Twitter to reach audiences throughout the world and get its message across. For example, analysis of 3,500 tweets of the once popular Twitter account @Palinfoen showed how it framed events including Shireen Abu Akleh's death in 2022, by describing Israeli actions as criminal while validating Palestinian resistance (Amer 2023, 3). The account along many more Hamas-affiliated accounts have been blocked by social media administrators which has forced Hamas to search for alternative communication channels.

The primary accomplishment of this time involved developing propaganda content which focused on specific audiences. The organization uses strategic methods to create a "hybrid media system" which includes official outlets and privately-owned but controlled agencies to reach various audience segments including Israelis, Palestinians in Gaza and the West Bank, global Muslim communities and Western public (Zelkovitz and Limor 2025, 301, 302). For example, Hamas has conducted projective psychological warfare (PPW) against Israeli military personnel and citizens through their use of Hebrew media content including video recordings, street posters and musical compositions that used familiar songs to create fear, while portraying Israeli society as helpless (Rubinstein-Shemer and Flamer 2023, 1). The songs “The end of hope” and ”You came to Gaza, you came to your death" stand as specific examples from this period as the group used their lyrics about to deter and create fear amongst Israelis enlisting in the military (Rubinstein-Shemer 2024, 2, 9). For Western audiences, Hamas has used English-language softer content, reduced their militant rhetoric and highlighted a different perspective focused on their Gaza governance and social service work to gain political support (Margolin 2020, 1077).

The October 7 attacks were Hamas’ peak of real-time information warfare, with propaganda operations being merged with the military operations, rather than appearing after the fact. For several years prior to the attack, Hamas’s military preparations were disguised as public propaganda. On the day of the assault, the propaganda offensive was launched in perfect sync with the physical attacks. Hamas immediately weaponized the Telegram messaging app as a real-time terror broadcast platform, which also filled the Israeli information vacuum during the first few hours of the attacks. The al-Qassam Brigades (AQB) used their Telegram channel to initiate the operation and then flooded

worldwide networks with content (Lucaides 2023). The group shared both video recordings of its military training sessions and unprocessed footage recorded by the body cameras of its fighters during the operation (Lucaides 2023). The strategy succeeded in creating a permanent online presence despite every attempt for control. Furthermore, the group continued to spread propaganda through various websites and Telegram channels which kept operating despite legal restrictions and inconsistent blocking of online platforms. The information blitz was amplified from different media outlets which operated as a complex network. For example, the pro-Hamas "Gaza Now" channel experienced fast growth because it operated as the main platform to distribute combat footage and disturbing content to its large user base (Lucaides 2023). Hamas managed to use various communication channels to deliver instant information which produced its most powerful psychological impact while it maintained complete control over the story from start to finish. The following events created an unprecedented "deluge of online propaganda and disinformation" which was reported as the most extensive ever recorded thus transforming the conflict into a "world war online" that brought together state and non-state actors who spread false information (Meyers and Frenkel 2023).

In the aftermath of the attack, Hamas adapted its propaganda strategy to the new phase of the conflict, most notably through the release of hostage media to the public. This way, digital content continued to serve as a tool which the group used to reach its political and psychological targets. For example, the Telegram channel of the organization revealed an advanced system for organizing hostage videos, including videos showing hostages alive and manipulative messages sent to family members (Yarchi 2025, 9). From the community clinics and cassette tapes to the encrypted, algorithmically amplified horror of October 7, Hamas’s journey reflects a complete integration of propaganda into its warfare, using every technological tool available to shrink the gap against a more powerful adversary.

4.3 Training

Hamas members were educated over time with the use of different means and methods, beginning with clandestine meetings in the 1990s and progressing to training using modern tools and digital resources. The group has run educational programs that teach its supporters modern asymmetric warfare skills through a mix of distance learning and

hands-on technical training, facilitated and funded many times with foreign support (Margolin and Levitt 2023, 5).

For decades, educational institutions served as core centers that imparted intellectual and technical instruction to individuals, in-person. The basic training curriculum of the group used physical manuals on how to make bombs and execute sabotage, as its main teaching tools (IDF editorial team 2014). The early 2000s marked a pivotal shift into the digital realm. For example, in 2008, Hamas started the "Get Ready" online program, which had video courses, including quizzes that taught its members about explosives, military tactics, and how to aim at target vehicles (Ratzlav-Katz 2008).

Hamas dedicated its efforts during the 2010s to develop expertise in drone technology and other advanced technological fields. Observing the successes of other Iranian-backed groups like Hezbollah, which used weaponized drones in Syria as early as 2016, Hamas began investing in its own drone program (Stalisnky and Sosnow 2017). The operators learnt how to convert commercial drones into surveillance systems which could also conduct destructive missions. The technical education received direct support from Iran and Hezbollah which accelerated its pace through their provision of essential training and resources (Warrick et al 2023).

The October 7 attack's scope and coordination are clear proof of this years-long, technologically oriented educational process. For such a well-organized, multi-pronged attack, fighters needed to know more than just basic warfare. They also needed to know how to coordinate units, plan complex operations, and use specialist technical skills. The event was the violent conclusion of a generation of militants who had been educated through this evolving system.

The physical infrastructure of Gaza suffered total destruction during the subsequent conflict which now presents the primary obstacle for Hamas to operate its educational programs. As the group seems to be assuming a new, more network-based structure (Ranstorp 2025, 24), it's safe to assume that the distributed educational approach that the organization first used for online education, secure digital communication, and secret training programs will be the basis for virtual militant training in the future.

4.4 Financing

Hamas's financial operations have evolved over time to use modern technology and create a flexible funding system vital for its social and military operations. In its early years, the organization relied on direct government support and connections for funding (U.S. Department of the Treasury 2022). The Iranian government and other government agencies provided important financial and operational support that helped Hamas with its social welfare programs and initial military operations (Human Rights Watch 2002, 97). Individuals and sympathetic groups including Gulf region donors and Western diaspora communities also made charitable donations. Furthermore, the Iraqi government made cash payments to families of militants during the Second Intifada, while providing extra assistance to the families of suicide bombers (Human Rights Watch 2002, 100). During this time, Qatar also gave Hamas major financial support, sending millions per year, while the group kept on its political operations in Qatar (Elbagir et al. 2023). Notably, Israeli leaders backed the Qatari financial pipeline and used it to avoid collapse in Gaza while keeping Hamas as a rival group to the Palestinian Authority (Elbagir et al. 2023).

Another, more recent and high-tech arm of Hamas' financial operations is the use of cryptocurrencies. Hamas started using cryptocurrencies in the late 2010s leveraging blockchain technology, which provided both privacy and decentralized network control. In early 2019, the Izz al-Din al-Qassam Brigades started a Bitcoin fundraising campaign, which included educational videos that showed people how to use public computers and foreign crypto exchanges to protect their identities (Wilder 2021). The group started using different Bitcoin addresses for each donor to hide where the funding was coming from (Wilder 2021). Research shows that cryptocurrency operated as the main financial system with Hamas having received $41 million in crypto donations between 2020 and 2023 and Palestinian Islamic Jihad (PIJ) receiving $93 million (Awasthi 2024, 7). The funds were not only received but also moved between affiliated militant groups via crypto wallets (Berwick and Talley 2023).

Moreover, Hamas's most important and cutting-edge innovation was setting up a secret global investment fund. Before October 7, Israeli and U.S. intelligence found a network of legitimate-looking businesses in Turkey, Sudan, Algeria, and the UAE (Becker and Scheck 2023). These companies, operating in sectors from construction and mining to real estate

and even chicken farming, generated hundreds of millions in profits that were quietly funneled back to Hamas (Becker and Scheck 2023). The operation received its funding from Trend GYO which operated as a Turkish real estate company listed on the Turkish stock exchange to create a corporate appearance that enabled financial transactions through international banking systems (Becker and Scheck 2023). U.S. Treasury officials calculated that the secret investment fund had between $400 million and $1 billion in assets that Hamas's top leaders controlled (Berwick and Talley 2023). Hamas maintained a complex financial portfolio which produced steady multiple revenue streams that stayed out of sight throughout the several years before the October 7 attacks. Finally, international authorities failed to take decisive action on discovered intelligence, which allowed the financial network to continue its operations (Becker and Scheck 2023).

The October 7 attacks and their aftermath forced Hamas to adopt both traditional and new funding methods to continue its operations. The U.S. Department of the Treasury in 2022 indicated that Iran along with Qatar-based facilitators continue to provide essential backing to the group through their traditional state support. Furthermore, pro-Hamas support networks now operate through Telegram and dark web platforms which provide them with better anonymity to raise funds and accept cryptocurrency donations (Awasthi 2024, 5). This evolution—from suitcase cash and state-sponsored aid to cryptocurrency wallets and multinational corporate holdings—demonstrates Hamas's strategic adaptability. Finally, the group seems to operate a resilient financial system which utilizes resources through an informal system used for transferring money outside of traditional banking called “hawala” (Harms 2025), blockchain systems (TRM Labs 2025) and global financial markets to meet its operational funding needs, despite facing a global counter-terrorism financial effort.

4.5 Weapons

Prior to being able to launch a coordinated multi-domain strike on October 7, Hamas evolved its technological military capabilities through a deliberate path that began with simple smuggling operations and moved on to local manufacturing of sophisticated weaponry. Three primary elements have influenced the path's evolution: external collaborations, necessity, and ongoing attempts to exploit vulnerabilities against an adversary with superior equipment.

The organization used direct attack tactics as its main military approach during its first years of operations. The group initiated its first military operations through hostage-taking and gun attacks which started in 1989 and achieved notoriety through their 1990s and 2000s attacks involving suicide bombings against Israeli civilian areas (Wilson Center 2023). The creation of the Yasin rocket-propelled grenade (RPG) was its first significant in-house military manufacturing accomplishment. Named after Sheikh Ahmed Yassin, the group's founder, this locally manufactured anti-tank weapon was unveiled in 2004 and was based on Soviet RPG-2 and RPG-7 designs (IICC 2007). Hamas employed the Yasin, to launch close-quarters attacks on armored vehicles and Israeli reinforced positions. The 1980's also marked the beginning of tunnel operations, which started as smuggling routes to move goods and weapons between Egypt and Gaza (Hecht 2014).

The takeover of Gaza by Hamas in 2007 led to the establishment of a blockade by Israel and Egypt which resulted in Hamas's weapons program moving toward greater strategic depth and collaboration with outside forces. The organization used its resources to construct an extensive underground network which hosted extensive military facilities and incorporated electricity systems, communication networks as well as various branches to support command functions, logistics and storage (Boldrini 2024, 2, 4, 5). Concurrently, Hamas renewed and strengthened its alliance with Iran. The alliance brought major changes with Iran providing Hamas with rocket designs and essential components which allowed the group to improve their rocket and drone systems' capabilities (Ranstorp, 2025, 22).

These capabilities merged into a hybrid playbook which Hamas honed during the time leading up to October 7. For example, the Palestinian factions established a joint operations room with Hamas in 2018 to execute coordinated rocket attacks which would overwhelm the Israeli Iron Dome air defense system (Ranstorp 2025, 22). The October 7 attacks started with a rocket assault which used thousands of projectiles including the Ayyash-250 rocket (Ranstorp 2025, 22). The ground assault used innovative low-tech methods together with military-grade equipment which had received modern modifications. For example, Hamas used commercial DJI drones and Zouari kamikaze drones to attack Israeli surveillance towers and armored vehicles as well as bulldozers and explosives along the high-tech border barrier with Israel (Ranstorp 2025, 22). The

attackers then infiltrated using motorcycles, paragliders and vehicles including a golf cart (Zegart 2023, 3).

In the ongoing conflict since October 7, Hamas has continued to deploy and adapt its mixed arsenal. The group operates with sophisticated anti-tank guided missiles (ATGMs) which include the Russian-made laser-guided Kornet system that creates a major danger for Israeli Merkava tanks (Trabelsy 2023). Its locally produced rockets, such as variants of the Yasin series, remain in use alongside improvised explosive devices (IEDs) and one-way attack drones. The extensive tunnel system maintained its strategic value because it enabled military forces to move through the area while providing protection to their personnel who could use these tunnels to hold hostages during operations (Cronin 2023, 34). Despite the major blows it received, Hamas hasn't stopped developing its innovative capabilities through various domains to maintain its long-term asymmetric fight against a superior conventional military.

4.6 Cyber intelligence and operations

The cyber operations of Hamas have evolved through a systematic process, which enhanced the group's cyber threat capability from negligible to a significant security threat. The organization developed cyber capabilities in over a decade, transitioning from rudimentary social engineering techniques to sophisticated espionage and offensive capabilities prior to the design and execution of the October 7 attack (Groppi and da Cruz Amador 2023).

Hamas began its cyber intelligence activities decades ago with the gathering of Open-Source Intelligence (OSINT) on Israel which progressively became more structured and extensive over time (Flamer 2023, 1174). In 2013, initial cyber-attacks employed basic techniques that effectively lured Israeli government officials safeguarding critical infrastructure through the use of pornographic material (Groppi and da Cruz Amador 2023). By 2015, the strategy became more sophisticated, involving the establishment of counterfeit Facebook profiles imitating attractive women in order to befriend IDF soldiers (Groppi and da Cruz Amador 2023). The cyber team utilized authentic photographs of women in real-life situations, enhancing their realism through interaction with Israeli news content and corporate and political information. The discussions ultimately transitioned to WhatsApp, where, under the pretense of exchanging private content, soldiers were

deceived into downloading malicious Android applications that granted Hamas access to their device cameras, microphones, and files. In 2017, an IDF soldier interviewed by BBC News indicated that these "honey traps" allegedly yielded minimal short-term intelligence benefits while posing significant security risks (BBC News 2017).

The group expanded its net by taking advantage of technological and popular cultural trends, demonstrating remarkable ingenuity. In 2018, Hamas operatives targeted IDF soldiers using a fitness application for joggers in high-risk areas and, independently, infiltrated army units watching the Football World Cup from their bases with a compromised application named "Golden Cup" (Groppi and da Cruz Amador, 2023). The tactic spread to the dating applications “Catch&See” and “GrixyApp” in 2020. The Israeli cybersecurity industry indicated that these attacks reached "new levels of sophistication" as the developers of malware employed stealth techniques, rendering their malware far more challenging to detect (Benjakob 2022). The cyber intelligence operations yielded intelligence that disclosed Israeli military installations and armored vehicles situated in southern Israel, aiding planners in developing their offensive plans (Benjakob 2022).
The military planning of Hamas incorporated its cyber and information operations during the period leading to the October 7 attacks. The ground assault used bulldozers and paragliders as low-tech methods to break through Israel's technologically advanced border defenses. On the cyber front, Palestinian militants gained access to more than forty surveillance cameras which monitored Israeli settlements near Gaza borders through hacking which revealed Israeli security weaknesses and allowed them to monitor settlement activities before the attack (Groppi and da Cruz Amador 2023). The attackers began their digital assault which ran parallel to their physical assault on October 7. The distributed denial-of-service (DDoS) attacks began less than ten minutes following the first rocket launch to attack Israeli websites which provided critical public alerts about rocket attacks (Mimran 2023). The attacks reached their peak when attackers launched more than one million requests per second against civilian warning systems to cause disruptions. The hacktivist group AnonGhost which supports Hamas used the Red Alert rocket notification app vulnerability to distribute deceptive alerts which included a fake warning about a "nuclear bomb" (Mimran 2023). The group performed additional operations which included using its "BiBi" wiper malware to delete data from computer systems (Mimran 2023).

The cyber aspect of the conflict has extended to include multiple participants joining after the initial attack took place. The hacking groups supporting Palestine who allegedly received support from Iran and Russia through Cyber Av3ngers and Anonymous Sudan launched attacks against Israeli critical infrastructure including power distribution systems (Roussi and Miller 2023). Moreover, multiple different attack groups successfully interrupted many websites including the Jerusalem Post (Mimran 2023), with Israeli newspaper and media websites receiving more than half of all DDoS attacks followed by software companies and financial services (Yoachimik and Pacheco 2023). Most cyber-attacks against Israel caused minimal physical harm since the Israeli digital security systems did their job effectively but had major psychological effects on the population.

Chapter 5 - The technological transformation of Israel's war in Gaza

The October 7 Hamas's attack on Israel was a catastrophic intelligence and security failure due to several existing strategic, institutional and operational weaknesses. A flawed and enduring strategic idea was that Hamas was primarily deterred from a major conflict, more focused on the burdens of governing Gaza, and could be managed through economic measures such as permitting substantial Qatari financial transfers into the Gaza strip (Barnea 2024, 1070; Levite 2024). This helped create a policy environment where any Hamas military growth wasn't recognized as a major security threat. This assumption was also reinforced by the fact that Israel's political leadership maintained a dysfunctional relationship with the defense and intelligence establishment, namely dismissing vital warnings from the intelligence community about increasing Hamas's threats (Levite 2024; Wyss 2024, 2). Furthermore, the Israeli security services seemed to have been operating at maximum capacity because they needed to focus on the main threats such as the violence in the West Bank, Hezbollah operations and Iran (Wyss 2024, 3).

The Israeli military and intelligence community has faced a heated debate about the October 7 attack failures and the direction that it must take in the future (Salhani 2023; Wyss 2024, 1). On one side, critics argued about IDF's over-dependence on technology and identified the failure as stemming from misreading Hamas objectives due to excessive digital data collection while ignoring human intelligence (HUMINT) and ground-based

warning systems (Wyss 2024, 4; Barnea, 2025, 1070). It seems that there was a critical and persistent deficit in high-quality, HUMINT within the inner circles of Hamas's military and political leadership in Gaza (Barnea 2024, 1074). The Israeli intelligence agencies seemed to have failed to have trustworthy agents who could reveal Hamas's intentions and secret strategies, so they depended heavily on technical surveillance techniques, which included SIGINT, drone monitoring and digital communication tracking (Barnea 2024, 1073). Security analysis also presents a fundamental criticism which shows that Israeli intelligence made an error by not placing more emphasis on their analysis to understand Hamas' geopolitical and moral motivations while maintaining an incorrect belief that Hamas would be deterred (Barnea 2025, 1071). The over-reliance on technology allegedly created a critical situation where IDF lost sight of their operational security and placed their faith more in their physical and digital fortifications, like the multibillion-dollar Iron Wall with its underground sensors and the Iron Dome missile defense system and extensive surveillance networks. The belief that Israel controlled everything and was immune to harm resulted in major strategic choices which proved disastrous. The military force at the front lines became weaker because security resources were redirected from Gaza border protection to other areas, making the region more exposed to Hamas' successful low-tech ground assault tactics (Levite 2024). The solution according to the critics of this approach requires better data not more, namely more human-based analysis which understands enemy mental processes and operational thinking instead of over-relying on additional quantitative data.

However, the main Israeli institutional response has been a strong dedication to developing more advanced technological systems which will become more extensive and more highly integrated (Heilbrunn 2024). The defense establishment didn’t view the catastrophic attacks as a technological failure but a failure of implementation and scale. The current approach to conflict management stems from a doctrine first described by Major General Isaac Ben-Israel in the 1990s, which posits that Israel must drag conflicts into the high-technology domain where it holds an absolute edge (Heilbrunn 2024). Furthermore, the IDF has established its new five-year force-building plan which makes artificial intelligence, robotics, and autonomous systems essential for all military domains (Kraft 2025). At the same time, Israel's defense industry has publicly showcased a suite of new technologies battle-tested in Gaza, from AI-powered drone orchestration systems to unmanned ground vehicles and the new "Iron Beam" laser defense system, which it is

actively marketing for export (Levaton and Fabian 2025). Furthermore, the technological advancement depends on and receives increased support from Big Tech companies worldwide who provide cloud infrastructure and data processing capabilities for systems including "The Lavender" and "The Gospel". As one investigative report noted, the vision within Israel's elite Unit 8200 was to forge relationships with Silicon Valley akin to those with traditional defense contractors like Lockheed Martin (Yachot 2025).

5.1 The technologies that shape Israel’s war in Gaza

In the aftermath of October 7, Israel got involved in an unprecedented global information war, described as a "deluge of online propaganda and disinformation" (Myers and Frenkel 2023). Israel used advanced technological methods to fight Palestinian narratives, while defending its military operations in Gaza through a multi-channel strategy. Israel used covert communication operations as its primary method to achieve its goals. For example, the Ministry of Diaspora Affairs in Israel dedicated $2 million from its budget to fund political marketing services (Frenkel 2024). This effort utilized hundreds of fake accounts on X (formerly Twitter), Facebook, and Instagram that posed as Americans to post pro-Israel comments and target specific U.S. lawmakers. The operation used AI as its main instrument to create content through ChatGPT while it established fake news websites in English (Frenkel 2024). Furthermore, the official Israeli government and military social media accounts used X to control their narrative and directly accuse, when needed, major international news organizations, including the BBC and CNN, claiming they distributed Hamas propaganda (Banjo 2025).

Israel also tried to control the visual narrative through the use of powerful emotional and graphic content, focusing on the October 7 hostage situation. The videos and photographs of hostages were strategically distributed through sponsored content to create strong public reactions and preserve international backing (Banjo 2025). Israeli accounts simultaneously tried to fight against the overwhelming number of images of starvation coming from Gaza dismissing them as staged and at times employing the term "Pallywood". The Israeli counternarrative and propaganda was not limited to the Palestinian field but extended to other actors in the region. For example, the Israeli government saw an increase in AI-produced disinformation from pro-Iranian social media accounts which showed fake missile strikes against Tel Aviv and fake footage of Israeli fighter jets getting destroyed

while the videos received more than 10 million views. Pro-Israeli actors distributed their own deceptive information through social media by sharing outdated video footage which they presented as evidence of Iranian public opposition and through AI-created videos that pretended to show Iranian people chanting: "We love Israel" (Murphy, Robinson and Sardarizadeh 2025).

In the war that broke out after the attacks, the Israeli military started using Gaza as a testing ground for AI-based warfare operating at unprecedented speeds and handling massive data processing needs. The technological shift gained its strength from "The Studio" which IDF's Unit 8200 operated as an innovation hub through an undercover operation (Frenkel and Odenheimer 2025). In the days following October 7, reservists who were allegedly data scientists and AI engineers at leading U.S. tech companies were mobilized into “The Studio”. The team used their civilian knowledge to train large language models (LLMs) for processing extensive and complex datasets. The LLMs helped the team solve critical battlefield problems through a fast development process that combined Silicon Valley methods with military intelligence requirements (Frenkel and Odenheimer 2025). This entire effort was also powered by the immense computational infrastructure of “Project Nimbus”, a cornerstone $1.2 billion cloud computing contract with Google and Amazon. The project established its first local data centers in Israel during 2021 to store government and military information and the contract allegedly includes special terms making Google and Amazon unable to block service access or limit Israeli platform usage even when their terms of service could be violated (De Vynck 2025).

In IDF’s aerial surveillance operations, the combination of artificial intelligence with modern drone systems has brought a complete transformation. For example, the Eitan platform can operate for over 30 hours while having a 737 Boeing-like wingspan to provide continuous weather-independent surveillance of Gaza (Testa 2024). Furthermore, the IDF drone systems evolved from remote surveillance control to fully autonomous AI tracking which represents a key development. The drones use computer vision algorithms which enable them to track particular vehicles and people through visual identification and movement patterns instead of hovering over a fixed coordinate. The system provides operators with the ability to achieve "deadly precision" when they need to track moving targets throughout different areas in a challenging combat environment (Frenkel and

Odenheimer2025). Nonetheless, such automation contains an inherent risk because the drones' visual identification system depends on statistical models derived from its training data. The algorithm can effectively fail to distinguish combatants from civilians in Gaza's dense urban areas leading to incorrect target selections, with a speed that can exceed a human operator's ability to stop system errors from happening and intervene when needed (Düz 2025).

On the ground, the IDF rapidly set up military checkpoints that used facial recognition technology to screen Gazans. The practice grew a lot quickly thanks to years of development in the West Bank. The "Blue Wolf" and "Red Wolf" systems operated in Hebron and East Jerusalem to establish a detailed face recognition database which soldiers used at checkpoints for facial identification and population control (Testa 2025; Düz 2025). In Gaza, no such permanent infrastructure existed prior to the war. The post-October 7 program, reportedly using specialized software from the Israeli company Corsight and even the consumer-grade face-grouping algorithm in Google Photos, was built from the ground up (Andersin 2025; Frenkel 2024). The military established surveillance cameras which monitored Palestinians who attempted to escape south or travel through areas under IDF control. The system operates to identify people in public areas, before it searches their images against databases that contain information from social media platforms, official documents and Hamas internal records that Israeli forces extracted. The program started as a hostage search operation, but it evolved into a mission to detect Hamas and Palestinian Islamic Jihad suspects who tried to blend with non-combatant civilians (Frenkel 2024). The system has also generated false positive results during warzone operations when lighting and environmental conditions were poor and produced wrong matches between innocent people and wanted militants, which resulted in several cases of illegal arrest and questioning (Frenkel 2024).

To monitor the movement of Gaza's population and locate specific targets within Gaza's dense urban landscape, the IDF employs several data tracking systems. For example, the IDF used cell phone movement tracking as their main method to monitor large numbers of people. A tool monitored more than one million mobile devices to generate a real-time map which showed population distribution and monitored compliance with evacuation orders for northern Gaza to the south (Kingsley and Bergman 2023). This method can also produce unreliable results as it doesn’t deliver exact real-time positions of people and the

warzone environment with its power and communication blackouts makes the collected data even less trustworthy which could lead to incorrect conclusions about civilian presence. A more novel and perhaps controversial tool is an AI-powered audio geolocation system. The system uses background noises from intercepted phone calls to determine a speaker's location through the identification of sounds such as distant airstrikes, generators, or echoes. The system doesn't provide exact location data but suggests a possible area zone (Frenkel and Odenheimer 2025). This tool was reportedly used in the strike that killed Hamas commander Ibrahim Biari in October 2023. This system can also produce inaccurate results as it can only indicate a broad location within crowded city areas instead of showing exact apartment or room locations which led to numerous civilian deaths during that operation (Frenkel and Odenheimer 2025).

To analyze the massive volume of intercepted Palestinian communications, the Unit 8200 engineers created a special Arabic-language large language model which operated as an AI chatbot system. The AI system was trained based on Israel's extensive historical database which contains phone call intercepts, social media content and text messages written in Palestinian Arabic dialects (Frenkel and Odenheimer 2025). The system allows analysts to perform fast conversational searches through millions of data points and, for instance, analyze public sentiment after an airstrike, across different regions by scanning social media (Davies and Abraham 2025; Frenkel and Odenheimer 2025). The tool enables users to complete work that would normally require human linguists to spend weeks on the task. However, it is not infallible. The system fails to recognize contemporary slang terms while it struggles to decode coded language and English expressions which have been adopted from other languages. The system can also produce false information through "hallucination" as it can generate incorrect answers and summaries with certainty, which might direct analysts toward incorrect conclusions (Davies and Abraham 2025).

The most strategically consequential application of this technological acceleration includes a targeting ecosystem designed to generate military targets at an industrial scale and unprecedented pace. The core of this system is known with the name "Lavender" (Abraham 2024; Frenkel and Odenheimer 2025) In the early stages of the war, Lavender was used to analyze mass surveillance data and assign tens of thousands of Gazan men a numerical score indicating the algorithmic likelihood of being a member of Hamas or Palestinian Islamic Jihad. The IDF soldiers who accessed intelligence data reported that

Lavender created a target list which at times contained up to 37,000 people (Abraham 2024). Intelligence officers would determine the minimum score which would lead to designation, but the AI system applied wide-ranging conditions including militant group membership and frequent cell phone changes. Lavender would produce wrong identification results up to 10% of the time which would result in thousands of incorrect identity matches. Sources described a production-line process where, for low-ranking targets, human review was sometimes reduced to a mere 20-second verification, often just to confirm the target was male, before authorization for a strike (McKernan and Davies 2024; Abraham 2024). A companion system referred to as “Where’s Daddy?” would then monitor people that Lavender identified through its tracking system by using electronic signals to determine when they entered a specific location, usually their homes (Abraham, 2024; Düz 2025). The system which connected people to specific locations served as a tool that facilitated airstrikes but made operational convenience more important than military rules, thus ensuring that civilians casualties would occur when family members were in the area.

In Israel, it looks like the path forward keeps on betting on a technical arms race despite the vocal critiques against technological complacency. The current position of the Israeli security establishment suggests that the solution to technology limitations will not come from more high quality HUMINT, but from building an enhanced digital protection system which uses automated processes and large amount of data. Finally, the open question regarding Israel's future security is whether its fast-paced technological transformation will close the human-based analytical gaps which became apparent during the recent and ongoing crisis or if it will simply create a more efficient system that remains vulnerable to strategic misjudgment.

Conclusions

The thesis examined how non-state actors attempt to leverage technology to shrink the power gap against powerful state adversaries, using as case study Hamas and the protracted conflict with Israel. The research results demonstrate that modern warfare is undergoing a major transformation. The available evidence shows a self-perpetuating cycle where accessible innovation enables non-state actors to challenge effectively their state adversaries. In return, powerful states develop and test even more advanced and automated

military systems that transform worldwide security dynamics. The research uses the Hamas-Israel conflict as a case study that showed how Hamas implemented basic commercial technology to carry out the October 7 attacks and how Israel in return has intensified its arms race and used Gaza as the testing ground of high-tech military technology.

The research showed that non-state actors use practical ingenuity together with modern tools which are widely available to execute their strategy and carry out their operations. Without the means to build conventional armies, these groups systematically take advantage of inexpensive, dual-use digital and commercial technologies to perform every function they need. They use the online world as their main operational space for spreading propaganda, for radicalizing and recruiting through social media and encrypted apps, and for raising funds through cryptocurrencies and cyber-crime. The training process takes also place in virtual environments which use adapted commercial systems to deliver instructions while intelligence collection occurs through analysis of open-source data. The modern world has achieved significant technological advancements as drone components, 3D printing technology and encryption software have become accessible worldwide. Non-state actors now possess the ability to develop military capabilities which used to be reserved for states as they can acquire drones which enable them to attack vital infrastructure at a long range. Their innovation is not about matching state power head-on but about finding ways around it. It is safe to assume that the increasing sophistication of artificial intelligence systems will advance this development further by performing intricate operations independently creating new security and legal problems that current security frameworks cannot handle.

Hamas's trajectory represents a key example of this wider development where non-state groups use technology to level the playing field against powerful state adversaries. The group achieved its peak point when it transformed into a hybrid force that could operate basic technological systems effectively to plan and carry out the October 7 attacks. Hamas used tunnel networks together with commercial drones, encrypted communication systems and launched numerous basic rockets simultaneously to demonstrate how affordable innovative methods could overwhelm and strike effectively much more sophisticated defense systems. The October 7 attacks demonstrated that non-state actors can generate

strategic disasters through guile, their ability to find vulnerabilities in their enemies' highly superior military systems and using their enemy's technological complacency against them.

In the aftermath of the attacks, the conflict has accelerated a new phase of military development. The Israeli military technology sector has experienced accelerated development, and the Israeli state has been investing heavily into technological innovation supported by the development of new military doctrines which focus on AI, robotics and autonomous systems. This vision, forged in combat, is now a product being exported globally, as defense industries market these battle-tested innovations. This creates an obvious dangerous loop which starts with major attacks that lead states to spend more heavily on advanced technology which they later export globally to transform future military capabilities for both nations and their opposing forces.

During the Gaza war, Israel implemented AI and automation systems at a large scale for military operations converting the battlefield on Gaza into a testing ground. The conflict has featured various interconnected systems which employ AI capabilities to identify targets, perform surveillance using facial recognition systems, while drones function autonomously for reconnaissance and airstrikes. These systems require powerful computing resources which international big tech companies provide. With the goal of producing decisions which exceed human possible speed, such systems have multiple dangerous built-in risks. For example, making decisions extremely fast through automation can push vital human judgment and legal review out of the process. The unavoidable errors in any algorithm can lead directly to tragic misidentifications on the ground. Also, using AI in war invites enemies to find ways to trick, disrupt, or hack these automated systems.

Thus, the Israeli response establishes a fundamental contradiction: It attempts to resolve system failures through advanced technological solutions despite the fact that these failures result mainly from human knowledge deficiencies, poor strategic decisions and political errors. The situation has demonstrated a risky pattern which can generate dangerous effects spreading across the entire world. The ability of affordable versatile tools to support non-state groups can force states to develop even more advanced automated systems which cost more and more. This runs the risk that state organizations can lose their core strategic direction as they become preoccupied with obtaining a tactical edge through technology.

The research points to multiple critical domains which require additional study. Academics and diplomats may need to address the current ethical and legal framework which governs next-generation warfare with its autonomous targeting systems and AI-operated cyber-attacks. The durability of decentralized financial systems using cryptocurrency and the growing, essential role of big tech companies providing services and infrastructure to modern militaries present new and difficult security problems. Furthermore, the complete effects of war zone surveillance which uses mass monitoring together with AI-generated propaganda on human populations during long-term periods have not been determined.

The core issue which remains unsolved is whether technological progress will fix the core human and strategic challenges which asymmetric warfare continues to expose. The evidence from this conflict suggests that it cannot. Instead, it seems that a new and unstable balance is being set up where all sides are stuck in a cycle of action and reaction. In this era, technological innovation seems to be the main weapon and the biggest potential flaw. The organizations which will achieve a lasting advantage will be those that combine their ability to use technology effectively with human decision-making skills and deep knowledge of their opponents and their strategic planning abilities. Therefore, the side which understands its technological weaknesses and stays flexible to prevent its weaknesses from being exploited may determine the future of warfare.

Bibliography

Abraham, Yuval. 2024. "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza." +972 Magazine, April 3, 2024. https://www.972mag.com/lavender-ai-israeli-army-gaza/.

Alexe, Daria. 2025. "Neo-Nazi Exploitation Online: AI Voice-Cloning and the Revival of Hitler Speeches." GNET. November 21, 2025. https://gnet-research.org/2025/11/21/neo-nazi-exploitation-online-ai-voice-cloning-and-the-revival-of-hitler-speeches/.

Al Raffie, Dina A. 2025. "Comparative Intelligence Operations of Nonstate Armed Groups: A Comprehensive Review." Intelligence and National Security, 1–25. https://doi.org/10.1080/02684527.2025.2548157.

Amer, Mohammedwesam. 2023. "Hamas in Cyberspace: Social Media and Forms of Political Expression." Arab Media & Society, no. 35 (Winter/Spring 2023): 1-30. https://doi.org/10.70090/MA23HCSM.

Andersin, Emelie. 2025. "Military Use of Biometrics Series – Israel's Use of AI-DSS and Facial Recognition Technology: The Erosion of Civilian Protection in Gaza." Lieber Institute West Point. October 24, 2025. https://lieber.westpoint.edu/israels-use-ai-dss-facial-recognition-technology-erosion-civilian-protection-gaza/.

Awasthi, Soumya. 2024. "The Dark Web as Enabler of Terrorist Activities." ORF Issue Brief no. 717, 1-20. Observer Research Foundation. July 1, 2024. https://www.orfonline.org/public/uploads/posts/pdf/20240701105925.pdf.

Banjo, Damilola. 2025. "Israel's PR Spin Intensifies to Counter Global Outrage Over Gaza." PassBlue, August 13, 2025. https://passblue.com/2025/08/13/israel-heightens-its-social-media-campaign-to-counter-global-outrage-over-gaza/.

Barnea, Avner. 2024. "Israeli Intelligence Was Caught Off Guard: The Hamas Attack on 7 October 2023—A Preliminary Analysis." International Journal of Intelligence and CounterIntelligence 37 (3): 1056–1082. https://doi.org/10.1080/08850607.2024.2315546.

BBC News. 2017. "Israeli soldiers 'caught in Hamas online honey trap'." January 12, 2017. https://www.bbc.com/news/world-middle-east-38594669.

Beccaro, Andrea. 2022. "Non-State Actors and Modern Technology." Small Wars & Insurgencies 34 (4): 780–802. https://doi.org/10.1080/09592318.2022.2104298.

Becker, Jo, and Justin Scheck. 2023. "Israel Found the Hamas Money Machine Years Ago. Nobody Turned It Off." The New York Times. December 16, 2023. https://www.nytimes.com/2023/12/16/world/europe/israel-hamas-money-finance-turkey-intelligence-attacks.html.

Benjakob, Omer. 2022. "Exposed Hamas Espionage Campaign Shows New Levels of Sophistication." Haaretz, April 7, 2022. https://www.haaretz.com/israel-news/tech-news/2022-04-07/ty-article/.premium/exposed-hamas-espionage-campaign-shows-new-levels-of-sophistication/00000180-5b9c-dc66-a392-7fdf14ff0000.

Berwick, Angus, and Ian Talley. 2023. “Militants Behind Israel Attack Raised Millions in Crypto.” The Wall Street Journal, October 10, 2023. https://www.wsj.com/world/middle-east/militants-behind-israel-attack-raised-millions-in-crypto-b9134b7a.

Boldrini, Chiara. 2024. "Hide and Seek, Hide and Fire: Hamas and the Tunnel Threat." Techreport, The Square, Insight #27, April 12, 2024. https://www.thesquared.it/en/product/hide-and-seek-hide-and-fire-hamas-and-the-tunnel-threat-insight-27/.

Busch, Etienne, and Jacob Ware. 2023. "The Weaponization of Deepfakes: Digital Deception on the Far-Right." The International Centre for Counter-Terrorism, October 26, 2023. https://doi.org/10.19165/2023.2.07.

Carchidi, Vincent. 2023. "The October 7 Hamas Attack: An Israeli Overreliance on Technology?" Middle East Institute (blog). October 23, 2023. https://mei.edu/publication/october-7-hamas-attack-israeli-overreliance-technology/.

Chen, Tianxia. 2012. “Exploration of the Hamas Suicide Attacks.” Journal of Middle Eastern and Islamic Studies (in Asia) 6, no. 2: 106-120. https://doi.org/10.1080/19370679.2012.12023205.

Choi, David. 2016. “An Inside Look at a Terrorist Group’s Summer Camp for Kids.” Business Insider, August 3, 2016. https://www.businessinsider.com/hamas-kid-summer-camp-2016-8.

Cronin, Audrey Kurth. 2006. "Cyber-Mobilization: The New 'Levée en Masse'." Parameters 36 (2): 77–87. https://doi.org/10.55540/0031-1723.2304.

Cronin, Audrey Kurth. 2023. "Hamas’s Asymmetric Advantage: What Does It Mean to Defeat a Terrorist Group?" Foreign Affairs 103, no. 1 (January/February 2024): 76-

91. https://www.foreignaffairs.com/israel/hamas-asymmetric-advantage-gaza-cronin.

Dass, Rueben. 2024. "Islamic State-Khorasan Province's Virtual Planning." Lawfare. October 24, 2024. https://www.lawfaremedia.org/article/islamic-state-khorasan-province-s-virtual-planning.

Dass, Rueben. 2025. "The Growing Threat of 3D-Printed Firearms in Far Right Networks." Center for the Study of Hate & Extremism. August 26, 2025. https://www.csohate.org/2025/08/26/3d-printed-firearms-in-far-right-networks/.

Dass, Rueben. 2025. "Gen-Zs and Ghost Guns: Trends, Threats and Implications." GNET (blog). September 24, 2025. https://gnet-research.org/2025/09/24/gen-zs-and-ghost-guns-trends-threats-and-implications/.

Dass, Rueben, and Abdul Basit. 2025. "Nascent Adoption: Emerging Tech Trends by Terrorists in Afghanistan and Pakistan." GNET. June 18, 2025. Accessed November 28, 2025. https://gnet-research.org/2025/06/18/nascent-adoption-emerging-tech-trends-by-terrorists-in-afghanistan-and-pakistan/.

Davies, Harry, and Yuval Abraham. 2025. "Revealed: Israeli Military Creating ChatGPT-Like Tool Using Vast Collection of Palestinian Surveillance Data." The Guardian, March 6, 2025. https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance.

De Vynck, Gerrit. 2025. "Google Rushed to Sell AI Tools to Israel's Military after Hamas Attack." Washington Post, January 21, 2025. https://www.washingtonpost.com/technology/2025/01/21/google-ai-israel-war-hamas-attack-gaza/.

Drăgan, Ioan M. 2024. "Lessons Learned about Radicalization: The Case of Hamas Radicalization Campaign and the New Wave of Extremism." National Security and the Future 25, no. 2: 227–72. https://doi.org/10.37458/nstf.25.2.8.

Düz, Sibel. 2025. "Gaza as a Testing Ground: Israel's AI Warfare." SETA Foundation, July 3, 2025. https://www.setav.org/en/gaza-as-a-testing-ground-israels-ai-warfare.

Elbagir, Nima, Barbara Arvanitidis, Alex Platt, Ebrahim Razek, Nadeen Raja, Uri Blau, and Shomrim. 2023. "Qatar Sent Millions to Gaza for Years – with Israel's Backing. Here's What We Know about the Controversial Deal," CNN. December

12, 2023.https://edition.cnn.com/2023/12/11/middleeast/qatar-hamas-funds-israel-backing-intl.

Eydoux, Thomas. 2022. "How Rebel Fighters Are Using 3D-Printed Arms to Fight the Myanmar Junta." FRANCE 24 Observers. Last modified January 11, 2022. https://observers.france24.com/en/asia-pacific/20220114-3d-printed-weapons-myanmar-rebels.

Firdous, Iftikhar. 2024. "ISKP Begins Publishing Pashto News Bulletins Using Artificial Intelligence." The Khorasan Diary (blog). May 21, 2024. https://www.thekhorasandiary.com/en/2024/05/21/iskp-begins-publishing-pashto-news-bulletins-using-artificial-intelligence/.

Flamer, Netanel. 2023. "'The Enemy Teaches Us How to Operate': Palestinian Hamas Use of Open Source Intelligence (OSINT) in Its Intelligence Warfare Against Israel (1987-2012)." Intelligence and National Security 38 (7): 1171–1188. https://doi.org/10.1080/02684527.2023.2212556.

Freilich, Charles D. 2017. "Israel's Counter-Terrorism Policy: How Effective?" Terrorism and Political Violence 29, no. 2: 359–376. https://doi.org/10.1080/09546553.2015.1044602.

Frenkel, Sheera. 2024. "Israel Deploys Expansive Facial Recognition Program in Gaza." New York Times, March 27, 2024. https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html.

Frenkel, Sheera. 2024. "Israel Secretly Targets U.S. Lawmakers With Influence Campaign on Gaza War." The New York Times, June 5, 2024. https://www.nytimes.com/2024/06/05/technology/israel-campaign-gaza-social-media.html.

Frenkel, Sheera, and Ben Hubbard. 2019. "After Social Media Bans, Militant Groups Found Ways to Remain." The New York Times, November 8, 2019. https://www.nytimes.com/2019/11/08/technology/terrorist-groups-social-media.html.

Frenkel, Sheera, and Natan Odenheimer. 2025. "Israel's A.I. Experiments in Gaza War Raise Ethical Concerns." New York Times, April 25, 2025. https://www.nytimes.com/2025/04/25/technology/israel-gaza-ai.html.

Gentry, John A. 2016. "Toward a Theory of Non-State Actors' Intelligence." Intelligence and National Security 31 (4): 465–89. https://doi.org/10.1080/02684527.2015.1062320.

Groppi, Michele, and Vasco da Cruz Amador. 2023. “Technology and Its Pivotal Role in Hamas’s Successful Attacks on Israel.” Global Network on Extremism & Terrorism (GNET). October 20, 2023. https://gnet-research.org/2023/10/20/technology-and-its-pivotal-role-in-hamass-successful-attacks-on-israel/.

Handler, Simon. 2022. “The 5×5—Non-State Armed Groups in Cyber Conflict.” Atlantic Council. Last modified June 28, 2022. https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-non-state-armed-groups-in-cyber-conflict/.

Harms, John. 2025. “Unmasking the Financial Lifelines of Terrorism.” Quantexa Blog, November 6, 2025. https://www.quantexa.com/blog/unmasking-the-financial-lifelines-of-terrorism/.

Hecht, Eado. 2014. "Gaza: How Hamas tunnel network grew". BBC. July 22, 2014. https://www.bbc.com/news/world-middle-east-28430298.

Heilbrunn, Ran. 2024. "The IDF's Cult of Technology: The Roots of the October 7 Security Disaster." American Affairs VIII, no. 3 (Fall 2024). https://americanaffairsjournal.org/2024/08/the-idfs-cult-of-technology-the-roots-of-the-october-7-security-disaster/.

Hroub, Khaled. 2017. “A Newer Hamas? The Revised Charter.” Journal of Palestine Studies 46 (4): 100–111. https://doi.org/10.1525/jps.2017.46.4.100.

Human Rights Watch. 2002. “Erased in a Moment: Suicide Bombing Attacks Against Israeli Civilians”. New York: Human Rights Watch. https://www.hrw.org/reports/2002/isrl-pa/ISRAELPA1002.pdf.

IDF Editorial Team. 2024. "Captured Intel Reveals Hamas' Explosive Plans." Israel Defense Forces. June 29, 2024. https://www.idf.il/en/mini-sites/hamas/captured-intel-reveals-hamas-explosive-plans/.

Intelligence and Terrorism Information Center at the Israel Intelligence Heritage & Commemoration Center (IICC). 2007. “Hamas’s Military Buildup in the Gaza Strip.” April 10, 2007. https://web.archive.org/web/20090117184057/http://www.terrorism-info.org.il/malam_multimedia/English/eng_n/pdf/hamas_080408.pdf.

Intelligence and Terrorism Information Center at the Israel Intelligence Heritage & Commemoration Center (IICC). 2007. “Palestinian children playing with plastic weapons, copying the fighting methods of the terrorist organizations.” November, 8, 2007. https://www.terrorism-info.org.il/Data/pdf/PDF_07_242_2.pdf.

Jenkins, Brian Michael. 2011. “Is Al Qaeda’s Internet Strategy Working?.” RAND Corporation. https://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT371.pdf.

Johnston, Trevor, Erik E. Mueller, Irina A. Chindea, Hannah Jane Byrne, Nathan Vest, Colin Clarke, Anusree Garg, and Howard J. Shatz. 2023. “Countering Violent Nonstate Actor Financing: Revenue Sources, Financing Strategies, and Tools of Disruption.” RAND Corporation. https://www.rand.org/pubs/research_reports/RRA687-1.html.

Kingsley, Patrick, and Ronen Bergman. 2023. "Tracking Cellphone Data by Neighborhood, Israel Gauges Gaza Evacuation." New York Times, October 16, 2023. Updated October 18, 2023. https://www.nytimes.com/2023/10/16/world/middleeast/gaza-invasion-israel-cellphone-data.html.

Kraft, Dina. 2025. "How Israel Failed to Anticipate Hamas: Intel Trusted Tech Over People." The Christian Science Monitor, March 12, 2025. https://www.csmonitor.com/World/Middle-East/2025/0312/israel-hamas-intelligence-failure-technology.

Kurtulus, N. Ersun. 2012. "The New Counterterrorism: Contemporary Counterterrorism Trends in the United States and Israel." Studies in Conflict & Terrorism 35 (1): 37–58. https://doi.org/10.1080/1057610x.2012.631456.

Levaton, Stav, and Emanuel Fabian. 2025. "Defense Ministry Hands IDF First Combat-Ready Iron Beam Laser Interception System." The Times of Israel, December 28, 2025. https://www.timesofisrael.com/defense-ministry-hands-idf-first-combat-ready-iron-beam-laser-interception-system/.

Levite, Ariel (Eli). 2024. "How Was Israel Caught Off-Guard?" War on the Rocks, February 22, 2024. https://warontherocks.com/2024/02/how-was-israel-caught-off-guard/.

Levitt, Matthew. 2007. Teaching Terror: How Hamas Radicalizes Palestinian Society. Policy Focus No. 60. Washington, DC: The Washington Institute for Near East

Policy. Published February 12, 2007. https://www.washingtoninstitute.org/pdf/view/7782/en.

Levy, Ido. 2024. “How Hamas Built an Army.” The Washington Institute for Near East Policy. January 2, 2024. https://www.washingtoninstitute.org/pdf/view/18557/en.

Listek, Vanesa. 2024. “3D printing Terror? New Study Highlights Right-Wing Extremists’ Use of 3D Printed Guns.”3DPrint.com, July 19,2024. https://3dprint.com/311150/d-printing-terror-new-study-highlights-right-wing-extremists-use-of-3d-printed-guns/.

Lucaides, Darren. 2023. “Telegram, Hamas, and the War for Information.” Wired. October 31, 2023. https://www.wired.com/story/telegram-hamas-israel-conflict/.

Mair, David. 2016. “#Westgate: A Case Study: How al-Shabaab Used Twitter during an Ongoing Attack.” Studies in Conflict & Terrorism 40 (1): 24–43. https://doi.org/10.1080/1057610X.2016.1157404.

Margolin, Devorah. 2020. “#Hamas: A Thematic Exploration of Hamas’s English-Language Twitter”. Terrorism and Political Violence 34, no. 6 (2020): 1076–1101. https://doi.org/10.1080/09546553.2020.1761343.

Margolin, Devorah, and Matthew Levitt. 2023. "The Road to October 7: Hamas' Long Game, Clarified." CTC Sentinel 16, no. 10 (October/November): 3-13. https://ctc.westpoint.edu/wp-content/uploads/2023/11/CTC-SENTINEL-102023.pdf.

McKernan, Bethan, and Harry Davies. 2024. “‘The Machine Did It Coldly’: Israel Used AI to Identify 37,000 Hamas Targets.” The Guardian, April 3, 2024. https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes.

Mimran, Tal. 2023. "Cyberspace: A Hidden Aspect of the Conflict." Lieber Institute West Point, November 30, 2023. https://lieber.westpoint.edu/cyberspace-hidden-aspect-conflict/.

Mozes, Tomer, and Gabriel Weimann. 2010. “The E-Marketing Strategy of Hamas.” Studies in Conflict & Terrorism 33 (3): 211–225. https://doi.org/10.1080/10576100903555762.

Myers, Steven Lee, and Sheera Frenkel. 2023. “In a Worldwide War of Words, Russia, China and Iran Back Hamas.” The New York Times. November 3, 2023.

https://www.nytimes.com/2023/11/03/technology/israel-hamas-information-war.html.

Murphy, Matt, Olga Robinson and Shayan Sardarizadeh. 2025. "Israel-Iran Conflict Unleashes Wave of AI Disinformation." BBC News. June 21, 2025. https://www.bbc.com/news/articles/c0k78715enxo.

Nelu, Clarisa. 2024. "Exploitation of Generative AI by Terrorist Groups." International Centre for Counter-Terrorism (ICCT). June 10, 2024. https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

Ogele, Eziho Promise. 2024. "The Intersection of Gaming and Terrorism: Exploring the Role of Online Gaming in Terrorist Recruitment Methods." Political Observer Portuguese Journal of Political Science | Revista Portuguesa de Ciência Política, no. 22: 23–39. https://doi.org/10.59071/2795-4765.RPCP2024.22/p 23-39.

Ortiz, Miguel. 2023. "3D-Printed Guns Are Being Used in the Myanmar Civil War." We Are the Mighty. July 25, 2023. https://www.wearethemighty.com/tactical/3d-printed-guns-are-being-used-in-the-myanmar-civil-war/.

Paul, T. V. 2007. "How the Weak Win Wars: A Theory of Asymmetric Conflict." Perspectives on Politics 5 (1): 203–204. https://doi.org/10.1017/s1537592707070624.

Primitivi, Manuel Nicola. 2024. “Anti-Junta Rebels Resort to 3D-Printed Weapons in Myanmar.” Jamestown, Military & Security, May 6, 2024. https://jamestown.org/anti-junta-rebels-resort-to-3d-printed-weapons-in-myanmar/.

Ranstorp, Magnus. 2025. "Inside Hamas: How It Thinks, Fights, and Governs." CTC Sentinel 18 (7): 16–28. https://ctc.westpoint.edu/wp-content/uploads/2025/07/CTC-SENTINEL-072025_article-3.pdf.

Ratzlav-Katz, Nissan. 2008. "Hamas Offering Online Courses in Jihad." Arutz Sheva/Israel National News, October 7, 2008. https://www.israelnationalnews.com/news/127904.

Reed, Alastair, and Haroro J. Ingram. 2017. "Exploring the Role of Instructional Material in AQAP’s Inspire and ISIS’ Rumiyah." In Proceedings of the 1st European Counter Terrorism Centre (ECTC) Conference on Online Terrorist Propaganda. The Hague: Europol. https://icct.nl/sites/default/files/import/publication/reeda_ingramh_instructionalmaterial.pdf.

Roussi, Antoaneta and Maggie Miller. 2023. “How Hackers Piled onto the Israeli-Hamas Conflict,” Politico. October 15, 2023. https://www.politico.com/news/2023/10/15/hackers-israel-hamas-war-00121593.

Rubinstein-Shemer, Niva. 2024. “‘Close but no Cigar’: Hamas’s Psychological Warfare against Israel between 2014 and 2023.” Middle Eastern Studies 61, no. 1 (2024): 1–17. https://doi.org/10.1080/00263206.2024.2355159.

Rubinstein-Shemer, Nesya, and Netanel Flamer. 2023. “Projective Psychological Warfare (PPW): An Analysis of Hamas Hebrew Videoclips as Part of Its Propaganda Campaign against Israel (2007–2014).” Middle Eastern Studies 60, no. 2 (2023): 336–350. https://doi.org/10.1080/00263206.2023.2186859.

Salhani, Justin. 2023. “Did Israel’s Overreliance on Tech Cause October 7 Intelligence Failure?” Al Jazeera, December 9, 2023. https://www.aljazeera.com/features/2023/12/9/did-israels-overreliance-on-tech-cause-october-7-intelligence-failure.

Shkolnik, Michael, and Alexander Corbeil. 2019. “Hezbollah’s ‘Virtual Entrepreneurs:’ How Hezbollah is Using the Internet to Incite Violence in Israel.” CTC Sentinel 12, no. 9 (October 2019): 28–35. https://ctc.westpoint.edu/wp-content/uploads/2019/10/CTC-SENTINEL-092019.pdf.

Stalinsky, Steven, and R. Sosnow. 2017. "A Decade Of Jihadi Organizations' Use Of Drones – From Early Experiments By Hizbullah, Hamas, And Al-Qaeda To Emerging National Security Crisis For The West As ISIS Launches First Attack Drones." MEMRI Jihad and Terrorism Threat Monitor Project. February 21, 2017. https://www.memri.org/jttm/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda.

Stockhammer, Nicolas. 2025. "From TikTok to Terrorism? The Online Radicalization of European Lone Attackers since October 7, 2023." CTC Sentinel 18 (7): 16–28. https://ctc.westpoint.edu/wp-content/uploads/2025/07/CTC-SENTINEL-072025_article-3.pdf.

Testa, Paola. 2024. “CLASSIFIED 1948/2024: What Israeli AI Implementation Teaches Us About the Warfare of Tomorrow.” GNET. March 18, 2024. https://gnet-research.org/2024/03/18/classified-1948-2024-what-israeli-ai-implementation-teaches-us-about-the-warfare-of-tomorrow/.

Thompson, Stuart A., and Mike Isaac. 2023. “Hamas Is Barred From Social Media. Its Messages Are Still Spreading.” The New York Times, October 18, 2023. https://www.nytimes.com/2023/10/18/technology/hamas-social-media-accounts.html.

Trabelsy, Nevo. 2023. "Israel Combats the Kornet Anti-Tank Missile." Globes. October 31, 2023. https://en.globes.co.il/en/article-israel-combats-the-kornet-anti-tank-missile-1001461332.

TRM Labs. 2025. “Category Deep-Dive: Use of Crypto in Terrorist Financing Expanded in 2024.” TRM Insights, March 5, 2025. https://www.trmlabs.com/resources/blog/category-deep-dive-use-of-crypto-in-terrorist-financing-expanded-in-2024.

U.S. Department of the Treasury. 2022. “Treasury Targets Covert Hamas Investment Network and Finance Official.” Press release. May 24, 2022. https://home.treasury.gov/news/press-releases/jy0798.

van Coller, Andrei. 2024. “Israel-Hamas 2024 Symposium – Qassam Rockets, Weapon Reviews, and Collective Terror as a Targeting Strategy.” Lieber Institute West Point. January 17, 2024. https://lieber.westpoint.edu/qassam-rockets-weapon-reviews-collective-terror-targeting-strategy/.

Warrick, Joby, Ellen Nakashima, Shane Harris, and Souad Mekhennet. 2023. "Hamas received weapons and training from Iran, officials say." The Washington Post. October 9, 2023. https://www.washingtonpost.com/national-security/2023/10/09/iran-support-hamas-training-weapons-israel/.

Wege, Carl Anthony. 2016. “Review of The Taliban’s Virtual Emirate: The Culture and Psychology of an Online Militant Community, by Neil Krishan Aggarwal.” International Journal of Intelligence and CounterIntelligence 30 (4): 833–837. https://doi.org/10.1080/08850607.2017.1337453.

Wesdorp, Daphne. 2023. "The Rebel Drone Maker of Myanmar." Wired. September 29, 2023. https://www.wired.com/story/the-rebel-drone-maker-of-myanmar/.

Wilder, Heidi. 2021."An Overview of the Use of Cryptocurrencies in Terrorist Financing." Coinbase (blog). September 21, 2021. https://www.coinbase.com/en-nl/blog/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing.

Wilson Center. 2023. "Palestinian Factions: Hamas and PIJ." The Islamists. November 3, 2023. https://www.wilsoncenter.org/article/palestinians-hamas-and-pij.

Winter, Charlie, Peter Neumann, Alexander Meleagrou-Hitchens, Magnus Ranstorp, Lorenzo Vidino, and Johanna Fürst. 2021. “Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies.” International Journal of Conflict and Violence 14 (March):1-20. https://doi.org/10.4119/ijcv-3809.