מכון ירושלים לאסטרטגיה ולביטחון
The Jerusalem Institute
for Strategy and Security

# Urban Guerrilla Warfare Conducted by Terrorist Organizations: Emerging Developments and Trends

Gabi Siboni
Simon Tsipsis

מכון ירושלים לאסטרטגיה ולביטחון
The Jerusalem Institute
for Strategy and Security

# Urban Guerrilla Warfare Conducted by Terrorist Organizations: Emerging Developments and Trends

Gabi Siboni
Simon Tsipsis

---

September 2025

# Urban Guerrilla Warfare Conducted by Terrorist Organizations: Emerging Developments and Trends

## 1. Introduction

Guerrilla warfare, urban warfare, terrorism, hybrid warfare, surrogate warfare and asymmetric warfare are terms that describe a range of methods and combat tactics used methodically against an opponent, with the goal of throwing him off balance. These tactics are common thanks to their simplicity, efficiency, and low resource-requirements. They pose significant challenges to states and regular armies forced to contend with them.

Industrial and technological revolutions have not bypassed these ancient methods. On the contrary, adoption of modern technologies has made these combat tactics even more efficient and popular, particularly in the past century and since the end of the Cold War. Transition to an era of limited, low-intensity conflicts has increased the use of urban and guerrilla warfare, as nearly every form of violent struggle—whether secessionist, anti-imperialist, ideological anarchy, racist-white supremacist, global criminal and drug-trafficking networks, political rebellion movements, terrorist organizations and "freedom fighters" —has employed these methods and applied a wide variety of irregular combat tactics.

Today, we can identify only short-term acute trends, whereas the next trend is already around the corner. In contemporary conflicts, insurgent and guerrilla groups employ technologies that are no less—and sometimes even more—advanced and effective than those possessed by the regular security forces fighting them. Their tools include cyber capabilities, artificial-intelligence systems, unmanned aerial vehicles, encrypted communications, extensive use of the internet and social-media platforms, and 3-D-printed weaponry. The use of technology by states increases their exposure to technology-based guerrilla warfare, for instance cyber hacking and disruption. Developments such as smart cities, expanding urban sprawl, consciousness influence and social opinion design operations, perception management, and psychological warfare challenge conventional methods of combat.

There are now many examples and lessons drawn from arenas of irregular, asymmetric, and hybrid warfare. This study seeks to examine and analyze the range of methods and components of modern guerrilla warfare. To that end, it surveys different conflict zones and innovations that present opportunities for regular state forces, with the aim of identifying advantages and shortcomings in dealing with the phenomenon of irregular guerrilla warfare in all its forms.

## 2. Urban Guerrilla Warfare

Guerrilla warfare—characterized by small, mobile groups using unconventional tactics such as ambushes, sabotage, and hit-and-run attacks against larger forces—has ancient roots. The Spanish word *guerrilla* ("little war") first appeared during the Peninsular War (1808–1814), but as a method of warfare it has a far longer history.

The earliest documented use of guerrilla tactics is attributed to Sun Tzu in *The Art of War* (sixth century B.C.E.), who advocated disrupting larger armies through mobility and surprise. Nomadic tribes such as the Scythians and Huns used similar methods against empires like Persia and Rome. In the third century B.C.E., the Roman general Quintus Fabius Maximus developed the Fabian strategy—avoiding direct battle with Hannibal during the Second Punic War—and earned the title of the "father of guerrilla warfare."[1]

The Bar Kokhba Revolt (132–136 C.E.) likewise relied heavily on guerrilla tactics. Bar Kokhba's fighters exploited the mountainous terrain and underground caves to cross combat zones, launch surprise attacks, and evade Roman forces, using their intimate knowledge of the terrain to their advantage.

During the Middle Ages and early modern period, guerrilla methods were employed by groups such as the Welsh against Norman invaders and by the Albanian leader George Kastrioti Skanderbeg against the Ottomans in the fifteenth century. In the seventeenth century, the Maratha leader Shivaji Maharaj pioneered Ganimi Kava —a form of guerilla warfare that employed cavalry raids, disruption of supply lines and use of terrain—against the Mughals, laying the groundwork for the Maratha Empire.[2]

Guerrilla warfare gained momentum through the eighteenth and nineteenth centuries—most notably in the American War of Independence (1775–1783), where militias used hit-and-run tactics against British forces, and in the Iberian Peninsula, where Spanish and Portuguese partisans harassed Napoleon's army and contributed to his first major continental defeat. It was there that the term *guerrilla* was coined. Later nineteenth-century struggles, such as the Dominican Restoration War (1863–1865) and the Boer Wars (1899–1902), again demonstrated the effectiveness of guerrilla strategies against colonial powers.[3]

---

[1] Joseph S. Roucek, "Guerrilla Warfare," *The Western Political Quarterly* 15, no. 1 (1962): 180–81; R. B. Asprey, "Guerrilla Warfare," *Encyclopedia Britannica*, August 8, 2025, https://www.britannica.com/topic/guerrilla-warfare.
[2] James Grant Duff, *The History of the Mahrattas* (Pickle Partners Publishing, 2014), 376.
[3] HubPages, "The Bloody History of Guerrilla Warfare," *HubPages*, October 3, 2023, https://discover.hubpages.com/education/Guerilla-Warfare-A-Brief-and-Bloody-Overview.

In the twentieth century, guerrilla warfare became a revolutionary instrument. The strategies of Mao Zedong in the Chinese Civil War (1930–1940) and Ho Chi Minh in the Vietnam War (1955–1975) illustrated their efficiency. The Yugoslav partisans under Tito during World War II further demonstrated their impact and effectiveness. The Cuban Revolution (1953–1959) led by Che Guevara and Fidel Castro made guerrilla tactics popular throughout Latin America.[4]

From 1944 to 1948, Menachem Begin, as commander of the Irgun (Etzel), was one of the key shapers of the concept of urban guerrilla warfare, formulating a strategy that emphasized striking at the prestige of the British Empire and undermining the Mandate. The strategy highlighted Britain's difficulty in coping with both guerrilla and terrorist tactics.

In South America, guerrilla warfare, rooted in movements such as the Cuban Revolution and Che Guevara's FOCO strategy of attrition by small, mobile cells, traditionally centered on rural revolt. The shift to urban settings and the integration of technology, however, changed these methods. The failure of rural campaigns and of military regimes' counter-operations in the 1960s–1970s led to models of urban insurgency in countries such as Argentina and Uruguay, which today integrate digital and technological tools.[5] Later, drug cartels and organized-crime networks throughout South America adopted this style of warfare, turning it into an effective and practical means of combat in the criminal sphere.

The guerrilla tactics used in Vietnam, which frustrated U.S. forces despite their technological superiority, remain a vivid example of how social, political, and environmental advantages can outweigh technological ones—a lesson that continues to hold in South America.[6]

Guerrilla warfare remains relevant in modern conflicts such as the Mujahideen resistance to the Soviets (1979–1989) in Afghanistan, the Taliban's fight against U.S. forces, and, of course, the actions of Hamas and other Palestinian terrorist groups in Gaza during the Swords of Iron operation, as well as in counterterrorism operations in Judea and Samaria. The success of guerrilla warfare often depends on local support, knowledge of terrain, and psychological factors, making it a durable strategy against superior forces.[7]

Historically, guerrilla movements such as those led by Che Guevara struggled to gain support from local peasants. Guevara's failed Bolivian campaign (1966–1967) showed that technology and weaponry alone cannot ensure success without a supportive

[4] Military Dispatches Editorial, "Understanding Guerrilla Warfare History: Strategies and Impacts," *Military Dispatches,* June 6, 2024, https://militarydispatches.com/guerrilla-warfare-history.
[5] Dirk Kruijt, "Che Guevara and Guerrilla Warfare," *Globalizations* 20, no. 8 (2022): 1528–1539.
[6] Sara Miles, "Why High-Tech Weapons Don't Work in Today's Low-Tech Wars," *WIRED*, December 6, 1996; Ronald H. Spector, "Firepower Comes to Naught," *Britannica*, August 14, 2025.
[7] Steven Metz, "Learning from Iraq: Counterinsurgency in American Strategy," *Strategic Studies Institute*, 2006.

environment.[8] In contrast, twenty-first-century conflicts that combine local support, advanced technology, and new weapons systems—supplied to separatist movements by one of the sides to the conflict—have achieved far more substantial results, including territorial annexations and the toppling of local regimes, as seen in operations by Russian-backed, pro-Moscow guerrilla forces in Ukraine.

## 2.1 The Impact of Urbanization and its Exploitation

The growth of large cities, especially in the global South, has created increasingly complex arenas of battle. In addition, smaller cities have emerged with excessive population density. Cities such as Sana'a, Mosul, and Gaza are characterized by extremely high population density, making conventional military operations in these urban centers costly, complex, and prone to cause collateral damage, including extensive civilian casualties and harm to urban infrastructure and social institutions.[9]

Prolonged urban conflicts, such as those in Aleppo or Gaza, involve siege tactics, aerial bombardment, and street fighting, all of which lead to severe humanitarian crises.[10] These crises are themselves one of the goals of urban guerrilla fighters: on the one hand, the devastated environment provides concealment and freedom of movement for militants and insurgents; on the other, humanitarian crisis creates leverage on the state to reach understandings, compromises, and concessions and to respond to the demands of guerrilla or terrorist organizations as was seen in case of Israel's Swords of Iron operation against Hammas terrorists in Gaza.

The urban environment supplies a form of "human disorder"—dense populations, large data pools, and extensive networks of relationships and communication—that masks guerrilla activity. Fighters blend into civilian populations and use urban infrastructure such as abandoned buildings, warehouses and containers, alleyways, structures, and tunnels for shelter and safe houses. An urban environment also provides effective mobility through a variety of accessible means of transport.[11]

Dense and expanding urban areas—such as the Gaza Strip, refugee camps, and the cities of Judea and Samaria in Israel's case, and similar densely populated areas in other places, from Africa to Latin America—offer clear tactical advantages for irregular warfare fighters. Tunnels, human shields, and close-quarters street fighting complicate conventional

[8] Barry Lando, "Latin-American Guerrillas," The Atlantic, December 1967; Dirk Kruijt, "Che Guevara and Guerrilla Warfare," *Globalizations* 20, no. 8 (2022): 1528–1539.
[9] *Focus Stratégique (IFRI)*, "The Future of Urban Warfare in the Age of Megacities," 2019.
[10] Pablo Villar Bolaños, "Lawyers, Guns and AI: Gaza's New Urban Warfare?" *Security Distillery*, July 26, 2024; also *Focus Stratégique (IFRI)*, "The Future of Urban Warfare in the Age of Megacities," 2019.
[11] Abbey Dorian, "Urban Guerrilla Warfare: The Threat of the Future?" *The Organization for World Peace*, 2019; see also *Military Dispatches Editorial*, "Urban Guerrilla Warfare: Strategies and Implications in Modern Conflict," June 11, 2024.

military operations and responses. Rising urbanization will spur greater use of urban terrorism and urban guerrilla warfare. As the trend of global urban growth intensifies, urban gangs and terrorist and guerrilla organizations will gradually prefer the urban arena. Hence, we are witnessing a hybridity between urban crime and city insurgencies, and irregular terrain military action.

However, the rise of smart cities, with networked sensors and pervasive surveillance, challenges traditional guerrilla tactics. Actions such as cutting power or disabling surveillance cameras to evade detection may trigger immediate alerts across these smart-city networks, allowing law-enforcement and security forces to respond almost instantly, thereby reducing the "anonymity" of guerrilla fighters and even leading to their capture. This notwithstanding, insurgents can exploit gaps in these systems, such as outdated infrastructure, or use cyberattacks on networks, to preserve operational effectiveness.[12]

Advanced technological tools create a degree of parity between guerrilla groups and state security forces. For example, drones allow small units to conduct surveillance or deliver payloads without direct engagement with security forces. In other words, adherence to traditional guerrilla tactics, combined with advanced technologies, enables the attainment of combat objectives with greater precision, lower risk of detection and fewer collateral effects and casualties among the militants.[13]

## 3. Technology and Combat Methods

The development of technology and the opportunities it offers have not bypassed terrorist and guerrilla groups, nor their activity in the urban arena. Although these features are not unique to the urban environment, this section provides a survey of how the arena is exploited in guerrilla warfare, as well as an examination of the various tools that urban guerrilla organizations use or can use.

### 3.1 Technological Tools

**Drones and robotics:** Terrorist groups increasingly use drones—UAVs, quadcopters, and other small, commercially available and inexpensive aerial vehicles—for reconnaissance, targeted attacks, and the transfer of weapons and explosives. For example, groups such as ISIS used drones in Iraq and Syria for surveillance and strikes, which improves their ability to operate in densely populated urban environments with minimal risk and inflicting maximal damage.[14]

[12] Anna M. Gielas, "Networked Sensors, Pervasive Surveillance, and AI-Powered Analytics: Urban Warfare in the Age of Smart Cities," *Modern War Institute*, July 2025.
[13] Michael Ashley, "From Muskets to Drones: Tech Is Transforming the Battlefield," *Forbes*, March 19, 2025.. https://www.forbes.com/sites/michaelashley/2025/03/19/from-muskets-to-drones-tech-is-transforming-the-battlefield.
[14] Marks, Thomas A., and Paul B. Rich. 2017. "Back to the Future – People's War in the 21st Century". Small Wars & Insurgencies 28 (3): 409–25. doi:10.1080/09592318.2017.1307620.

**Cyberwarfare:** Urban guerrilla fighters exploit vulnerabilities in computerized environments and systems used by authorities to operate smart-city infrastructure, carrying out actions such as hacking transportation systems or power-grid networks to disrupt urban activity. The integration of the Internet of Things (IoT) in smart cities creates potential for a new kind of attack against smart networks or surveillance systems. Guerrilla fighters also exploit digital blind spots or manipulate data to evade detection.[15] Cyberwarfare, the spread of disinformation, perception management, and misinformation operations have become an integral part of urban guerrilla warfare, with groups leveraging decentralized networks to spread propaganda or disrupt official narratives.

Use of AI is spreading: Guerrilla groups also leverage artificial intelligence (AI) for planning attacks, tracking and mapping, planting explosive charges, and coordinating movements by way of AI-based applications. Security forces, for their part, use AI-driven surveillance systems (for example, facial recognition) to contend with these threats, creating a technological arms race between urban terrorist organizations and security agencies. The integration of AI in counterterrorism operations will definitely increase; meanwhile, use of AI among terrorists and urban guerrilla fighters is also gaining momentum. At present, AI is applied mainly to the command and piloting of autonomous drones and to predictive-analytics devices.[16]

In addition, cyber terrorists widely use cyber warfare, by attacking and trying to penetrate state sensitive infrastructure targets to test government's reaction. This approach reflects tactics used by digital start-ups, in which hackers act as auxiliary forces to test the resilience of a software. By studying a state's reaction, cyber terrorists obtain a highly valuable insight and knowledge of state capabilities to improve its own skills and methods of offense and warfare. Terrorist groups employ similar methods to attack state infrastructure or carry out cyberattacks aimed at perception management, social narrative design, disrupting state control, and improving their own weapon systems.[17]

[15] Abbey Dorian. 2019. "Urban Guerrilla Warfare: The Threat Of The Future?". https://theowp.org/urban-guerrilla-warfare-the-threat-of-the-future; Also in Anna M. Gielas. 2025. "Networked Sensors, Pervasive Surveillance, and AI-Powered Analytics: Urban Warfare in the Age of Smart Cities". Modern War Institute, July. https://mwi.westpoint.edu/networked-sensors-pervasive-surveillance-and-ai-powered-analytics-urban-warfare-in-the-age-of-smart-cities.

[16] Anna M. Gielas. 2025. "Networked Sensors, Pervasive Surveillance, and AI-Powered Analytics: Urban Warfare in the Age of Smart Cities". Modern War Institute, July. https://mwi.westpoint.edu/networked-sensors-pervasive-surveillance-and-ai-powered-analytics-urban-warfare-in-the-age-of-smart-cities; Also in Pablo Villar Bolaños. 2024. "Lawyers, Guns and AI: Gaza´s New Urban Warfare?". Security Distillery . July 26, 2024. https://thesecuritydistillery.org/all-articles/lawyers-guns-and-ai-gazas-new-urban-warfare.

[17] Richard Robert. 2021. "Guerrilla 2.0: Asymmetric Warfare in the Tech Era". Polytechnique Insights, October 27, 2021. https://www.polytechnique-insights.com/en/braincamps/geopolitics/asymmetrical-warfare-new-strategies-on-the-battlefield/guerrilla-2-0-asymmetric-warfare-in-the-tech-era.

**Integration of physical and cyber operations:** Urban guerrilla fighters may also target critical infrastructure in smart cities—for example, water, sewage, electricity, gas, transportation, communication, and internet networks—by combining physical attacks with cyberattacks to maximize impact and cause the greatest possible disruption.[18]

**Encrypted communications:** Use of encrypted platforms such as WhatsApp and Telegram enables coordination, recruitment, and the relatively secure dissemination of propaganda and conduct misinformation campaigns while preserving decentralized command structures.[19] Modern guerrilla groups use encrypted messages and satellite communications to coordinate attacks, and they frequently use civilian technologies such as smartphones for secure communications.

**Advanced weaponry:** The spread of 3-D—printed weapons, mobile missile systems (on pickup trucks), and improvised explosive devices (IEDs) enables small groups to bring significant firepower to bear on field without relying on external arms suppliers and to bypass state enforcement mechanisms.[20] IEDs detonated by mobile phones or other civilian technologies have been adapted for use in terrorism and guerrilla warfare, combining cheap materials with advanced technological precision.[21]

**Artificial intelligence and surveillance:** Guerrilla groups leverage artificial intelligence to plan attacks, for example by using mapping applications to place explosive devices or to coordinate movements and actions. Security forces likewise use AI-driven surveillance systems (for example, facial recognition) to contend with these threats, which creates a technological arms race between urban terrorist organizations and security agencies.[22]

[18] Abbey Dorian. 2019. "Urban Guerrilla Warfare: The Threat of the Future?". https://theowp.org/urban-guerrilla-warfare-the-threat-?of-the-future; Also in Anna M. Gielas. 2025. "Networked Sensors, Pervasive Surveillance, and AI-Powered Analytics: Urban Warfare in the Age of Smart Cities". Modern War Institute, July. https://mwi.westpoint.edu/networked-sensors-pervasive-surveillance-and-ai-powered-analytics-urban-warfare-in-the-age-of-smart-cities.

[19] Richard M. Crowell. 2022. "Great Power Competition — China's Use of Guerrilla Warfare and Information Power in Pursuit of Its Epochal World Order". Small Wars Journal, February. https://smallwarsjournal.com/2022/07/02/great-power-competition-chinas-use-guerrilla-warfare-and-information-power-pursuit-its/#_ednref84.

[20] Everytown Research & Policy. 2025. "Printing Violence: Urgent Policy Actions Are Needed to Combat 3D-Printed Guns". Everytown Research & Policy, July 17, 2025. https://everytownresearch.org/report/printing-violence-urgent-policy-actions-are-needed-to-combat-3d-printed-guns.

[21] Richard Robert. 2021. "Guerrilla 2.0: Asymmetric Warfare in the Tech Era". Polytechnique Insights, October 27, 2021. https://www.polytechnique-insights.com/en/braincamps/geopolitics/asymmetrical-warfare-new-strategies-on-the-battlefield/guerrilla-2-0-asymmetric-warfare-in-the-tech-era.

[22] Anna M. Gielas. 2025. "Networked Sensors, Pervasive Surveillance, and AI-Powered Analytics: Urban Warfare in the Age of Smart Cities". Modern War Institute, July. https://mwi.westpoint.edu/networked-sensors-pervasive-surveillance-and-ai-powered-analytics-urban-warfare-in-the-age-of-smart-cities; Also in PABLO VILLAR BOLAÑOS. 2024. "Lawyers, Guns and AI: Gaza´s New Urban Warfare?". Security Distillery. July 26, 2024. https://thesecuritydistillery.org/all-articles/lawyers-guns-and-ai-gazas-new-urban-warfare.

## 3.2 Psychological Warfare and Social Networks

Social-media platforms amplify the narratives of guerrilla organizations and allow those organizations to recruit operatives globally. For example, ISIS accrued considerable "success" by using social media to recruit activists and to promote lone-actor attacks in Western cities.[23]

Guerrilla tactics such as hit-and-run attacks and sabotage are intended to instill fear and uncertainty both in authorities and among civilians. These actions do both: they undermine morale and create narratives for demand of security among society and cultivate resistance that resonate among local populations and gradually take root in in their minds.[24]

Use of social-media platforms for recruitment and for cognitive operations has increased, with terrorist actors exploiting open-source intelligence (OSINT) to plan attacks or to influence public opinion in the target state.

Guerrilla warfare often depends on local civilian support for resources, mobilization and intelligence collection and blurs the line between fighters and noncombatants. This dynamic—seen at times in conflicts such as the Syrian civil war, in the war in Ukraine, and of course in Judea and Samaria and Gaza—complicates military responses and increases the number of civilian casualties, thereby making it harder to achieve military objectives and prolongs the conflict gradually transforming it into a low- or a medium-intensity war of attrition. That prolongation is one of the guerrilla's war aims: to instill in the enemy's consciousness the belief that the campaign has no prospect of success and that it is preferable to grant guerrilla and terrorist groups their demands in order to bring the fighting to an end and return to a normal life.[25] The exhaustion of the public and security forces has become one of the main objectives in the era of irregular warfare, as this can exert pressure on government leadership both from within society and from the international community.

## 3.3 Methods of Operation

The use of sabotage and hit-and-run attacks in an urban environment enables small, mobile units of urban guerrilla fighters to carry out swift strikes and then withdraw into concealment within the urban surroundings. Many analysts of urban guerrilla warfare cite as examples the Palestinian *intifadas*, the wars in Gaza, and modern conflict in Syria.

---

[23] Laura Llach. 2023. "Lone Wolf Terrorists in Europe Are Not so Lonely Anymore - Who Is Radicalising and Recruiting Them?" October 26, 2023. https://www.euronews.com/2023/10/26/lone-wolf-terrorists-in-europe-are-not-so-lonely-anymore-who-is-radicalising-and-recruitin.

[24] Military Dispatches Editorial. 2024. "Urban Guerrilla Warfare: Strategies and Implications in Modern Conflict". Military Dispatches Editorial. June 11, 2024. https://militarydispatches.com/urban-guerrilla-warfare.

[25] S. Kalyanaraman. 2003. "Conceptualisation of Guerrilla Warfare". Strategic Analysis: A Monthly Journal of the IDSA, April. https://ciaotest.cc.columbia.edu/olj/sa/sa_apr03/sa_apr03kas01.html#:~:text=We%20fought%20a%20military%20war,the%20will%22%20of%20the%20adversary.

In addition to causing destruction, killing innocents, and spreading chaos and fear, the goal of organizations operating in an urban environment is to disrupt or paralyze critical infrastructure — electricity, transportation, medical care, heating systems and water supplies, , and other vital services — through deliberate sabotage intended to undermine the ability of law-enforcement and governing authorities to maintain control of the state.[26] Hence, another main goal of irregular warfare in the present era has become to collapse the state.

Inspired by guerrilla-warfare organizations and sometimes directly connected to them through assistance, preparation, and the provision of means and intelligence in advance of a terrorist attack, a lone attacker may serve as a cover for urban terrorist attacks carried out by urban guerrilla groups. ISIS provides a clear example of an entity that combines within itself both a terrorist organization and guerrilla warfare in open terrain — in the Middle East and Africa — and in urban environments such as the civil wars in Libya, Syria, Iraq, and elsewhere. It represents a hybrid terrorist entity. Inspired by groups like ISIS, lone-actors are carrying out "simple" attacks such as vehicle-ramming, stabbings, arson, and similar acts in urban centers.[27] If at first, during the inception of the Arab Spring, most of these attacks were carried out by genuine followers of Islamist ideologies, today irregular urban insurgent forces are widely using this tactic for much broader goals.

## 4. Case Studies

This chapter examines several case studies with the aim of identifying patterns of operation and enabling analysis of new operational templates used by terrorist actors, with an emphasis on Judea and Samaria and other theaters relevant to Israel.

### 4.1 Hamas in Gaza

Hamas operatives have integrated various forms of advanced technology into their guerrilla tactics against Israel. Hamas has adopted low-cost, accessible, and sometimes imported technologies to improve asymmetric actions, including ambushes, hit-and-run attacks, and prolonged subterranean activity. This allows it to offset conventional disadvantages through surprise, mobility, and psychological impact. The following is an overview of methods of operation in this theater, including use of technology.

[26] Military Dispatches Editorial. 2024. "Urban Guerrilla Warfare: Strategies and Implications in Modern Conflict". Military Dispatches Editorial. June 11, 2024. https://militarydispatches.com/urban-guerrilla-warfare.
[27] Focus Stratégique IFRI. 2019. "The Future of Urban Warfare in the Age of Megacities". https://www.ifri.org/en/studies/future-urban-warfare-age-megacities; Also in Muhammad Noor E Elahi Mirza, Irfan Ahmad Rana. 2024. "A Systematic Review of Urban Terrorism Literature: Root Causes, Thematic Trends, and Future Directions". Journal of Safety Science and Resilience 5 (3): 249–65. https://www.sciencedirect.com/science/article/pii/S2666449624000240.

### 4.1.1 Underground Tunnel Networks

Hamas's extensive tunnel system, referred to in the source as the "Gaza Metro," is a cornerstone of its guerrilla strategy and combines engineering and technology to enable sustained operations. The network extends for hundreds of kilometers, with tunnels equipped with electricity, ventilation, fuel supplies, communications systems, and landline telephones to ensure continuous communication during power outages or disruptions caused by IDF operations. These features enable Hamas fighters to move without being detected, to store weapons, and to carry out surprise attacks. The tunnels serve as launch points for ambushes, with shafts concealed inside civilian structures such as residential buildings, hospitals, mosques, schools, and UN facilities. The militants use them to evade aerial surveillance and to emerge for hit-and-run surprise attacks, often employing anti-tank missiles, mines, or sniper rifles. Advanced features include sensor-integrated booby traps, signaling tripwires, motion detectors, and acoustically triggered explosives designed to draw IDF soldiers into booby-trapped structures. Hamas has also developed remote-detonation capabilities using cameras to monitor and detonate charges at several sites simultaneously.

### 4.1.2 Rockets and Missiles

Hamas had an advanced self-production capacity until the Swords of Iron War was launched by the IDF. Part of it remains based on unexploded ordnance and improvised materials such as water pipes and on converting civilian raw materials for combat purposes.[28] Reliance on improvised rockets limits accuracy and sometimes causes civilian casualties or damage to civilian targets in the Gaza Strip and even causes casualties among Hamas fighters themselves.

Anti-tank weapons, including locally produced RPG launchers with shaped charges (for example, the al-Yassin 105), are used in short-range ambushes against armored vehicles. Imported systems, such as North Korean 7-F missiles or Libyan 103-AK rifles, increase firepower in urban skirmishes through the use of snipers and machine guns in urban combat. These upgrades allow Hamas to inflict damage without direct confrontation, in accordance with guerrilla principles of attrition.

### 4.1.3 Drones and Unmanned Aerial Vehicles

Hamas operated unmanned aerial vehicles (UAVs), usually home-made or supplied by Iran, to conduct reconnaissance, disrupt defenses, and attack Israeli forces with maximum precision. These drones represent a shift toward hybrid warfare, combining guerrilla tactics

[28] Ido Levy. 2024. "How Hamas Built an Army". The Washington Institute for Near East Policy, January. https://www.washingtoninstitute.org/policy-analysis/how-hamas-built-army; Also in AXIOS. 2023. "What to Know about Hamas' Military Capabilities". AXIOS. October 21, 2023. https://www.axios.com/2023/10/21/palestine-hamas-military-power.

with modern technology. Inexpensive commercial drones that underwent modification and/or upgrading are used to drop mortar shells or grenades on Israeli soldiers, turning improvised explosives into guided munitions.

Drones were deployed by a Hamas militants to strike IDF cameras, sensors, and communications towers, causing temporary blockage and blindness in IDF systems. Surveillance drones, combined with hidden cameras, enabled real-time monitoring of IDF movements and helped Hamas coordinate ambushes and time attacks, such as emerging from tunnels to fire RPGs or attach mines to IDF armored vehicles. Hamas use of drones has been basic but it could evolve to employment of swarms capable of slowing IDF advances on a large scale—making urban-guerrilla operations more effective and less predictable.

During the October 7 2023 attack, drones and even paragliders were used to breach the border fence with Israel, as drones dropped grenades.[29] These drones are basic—mostly commercially available or modified/upgraded models—and lack the technological sophistication of military-grade UAVs. Paragliders are inexpensive, difficult to detect by radar, and effectively exploit these gaps in Israel's defense systems.[30]

### 4.1.4 Cyber and Cognitive Operations

Hamas leverages digital platforms for psychological warfare. Although this is not unique to guerrilla activity in an urban arena, it is amplified in such an environment and increases the impact of guerrilla warfare beyond the battlefield. Hamas maintained (and, at the time of writing, perhaps still maintains) a dedicated cyber unit for espionage and disruption, which uses digital tools to support guerrilla operations in the field. These include malware and phishing against Israeli personnel and forces, fake social-media accounts, dating and fitness applications, and infected devices such as phones and USB drives, all of which are used to extract, steal, and collect data on the deployment of forces and military bases, troop movements, and blind spots.

Campaigns on social networks amplify narratives of Israeli oppression and glorify Hamas fighters, often sharing violent graphic content to influence public opinion.[31] Cyber operations are intended for intelligence gathering on Israeli targets, while propaganda serves to increase recruitment and international support. A campaign known as "Operation Broken Heart" used fake profiles to deceive IDF soldiers into downloading

[29] Michele Groppi, Vasco da Cruz Amador. 2023. "Technology and Its Pivotal Role in Hamas's Successful Attacks on Israel". Global Network of Extremism & Technology, October 20, 2023. https://gnet-research.org/2023/10/20/technology-and-its-pivotal-role-in-hamass-successful-attacks-on-israel; Also in defensemirror.com. 2023.
[30] Ibid.
[31] NBS News. 2014. "How Technology Is Intensifying Gaza War Between Israel and Hamas". NBS News, July 30, 2014. https://www.nbcnews.com/storyline/middle-east-unrest/how-technology-intensifying-gaza-war-between-israel-hamas-n158536.

spyware.[32] Hamas's cyber capabilities are relatively basic; there is no open evidence confirming sophisticated cyberattacks.

### 4.1.5 Surveillance and Intelligence Gathering

Hamas set up a covert aerial-surveillance system using high-quality cameras hidden in water-heating boilers, in order to monitor Israel's airspace.[33] The cameras were inexpensive but were positioned strategically, making use of everyday objects for concealment. The system provided Hamas with up-to-date information from the field and assisted in rocket launches and drone operations. The camera network deployed by Hamas is of unclear effectiveness, since Israel neutralized it relatively quickly. Claims about communications disruptions are mostly speculative and lack any evidentiary foundation.[34]

### 4.1.6 Improvised Explosive Devices and Anti-Tank Weapons

Hamas uses explosive charges, RPG-7 launchers, and home-made anti-tank rockets such as the Al-Banna, Al-Batar, and Al-Yassin to strike IDF forces. These weapons combine smuggled military equipment with locally produced versions. Explosive devices—both smuggled and domestically produced—are sometimes placed in buildings or in tunnels for use in ambushes. Explosive devices and anti-tank weapons enable Hamas to cope with IDF armored fighting vehicles and to carry out hit-and-run surprise attacks.[35]

## 4.2 Terror in Judea and Samaria

Terrorist activity in Judea and Samaria consists mainly of armed factions identified with groups such as Hamas, Palestinian Islamic Jihad (PIJ), Fatah's Al-Aqsa Martyrs' Brigades, and the Popular Front, together with local, cross-organizational frameworks such as the Jenin Brigades and Lion's Den in Nablus. These groups have integrated technology into their combat tactics in the urban arena, particularly since the Swords of Iron operation.

They employ improvised and smuggled systems to contend with Israel's technological superiority. Israeli security forces and agencies have identified a growing presence of locally produced arms and weapons smuggled from Iran, and the use of basic surveillance and coordination tools. The use of technology by these groups has been promoted by Iran whose goal is to arm them for the purpose of carrying out attacks on Israeli targets.[36]

---

[32] Daniel Byman, Emma McCaleb. 2023. "Understanding Hamas's and Hezbollah's Uses of Information Technology". https://www.csis.org/analysis/understanding-hamass-and-hezbollahs-uses-information-technology.
[33] defensemirror.com. 2023. "Weapons Used by Israel and Hamas in Gaza Conflict". Defensemirror.Com. October 14, 2023. https://www.defensemirror.com/feature/76/Weapons_Used_by_Israel_and_Ham as_in_Gaza_Conflict.
[34] defensemirror.com. 2023. "Weapons Used by Israel and Hamas in Gaza Conflict". Defensemirror.Com. October 14, 2023. https://www.defensemirror.com/feature/76/Weapons_Used_by_Israel_and_Ham as_in_Gaza_Conflict.
[35] New York Times. 2024. "Hamas's Guerrilla Tactics in North Gaza Make It Hard to Defeat". New York Times, October 22, 2024. https://www.nytimes.com/2024/10/22/world/middleeast/hamas-israel-gaza-guerrilla.html.
[36] James Mackenzie, and Ali Sawafta. 2025. "Israel Launches 'significant' Military Operation in West Bank, at Least 9 Palestinians Killed". Reuters, January 21, 2025. https://www.reuters.com/world/middle-east/israeli-military-begins-operation-west-bank-city-jenin-2025-01-21.

The organizations rely primarily on explosives, rockets, and ground-based weapons that are often hidden in the refugee camps.[37]

The terrorists in Judea and Samaria have adopted a combination of simple technological improvisations and advanced imported systems. The attempt to copy capabilities from Gaza to Judea and Samaria also includes efforts to integrate drones. There are reports of the use of basic drones for reconnaissance and intelligence purposes, although the evidence is scant in Judea and Samaria compared with Gaza.[38]

A significant portion of these technologies is acquired through smuggling networks run by Iran's Quds Force and Unit 4000, often via Jordan or Syria, with weapons concealed in shipments destined for areas such as Jenin.[39] Local production—such as the Al-Ghul rifle and Al-Yassin rockets—demonstrates growing self-reliance, inspired by Hamas's innovations in Gaza.[40]

Since 2023, there has been a significant increase in the amount of weapons possessed by the Palestinian groups in Judea and Samaria, despite IDF actions that thwarted Iranian schemes of supply of advanced equipment.[41] IDF raids in Jenin and Tulkarm in 2024–2025 revealed increased use of these weapons and technologies, leading to clashes in which gunmen caused casualties using RPG and explosive charges.[42] Below is a review of the principal uses of technology in the sector.

### 4.2.1 Explosive Charges and Improvised Devices

Improvised explosive devices and Claymore-type charges are widely used for ambushes and roadside attacks. The terrorists employ heavy explosives, including versions of anti-personnel and anti-vehicle mines such as explosively formed penetrators (EFPs), which are often fitted with wireless firing systems for remote detonation.[43]

---

[37] Jazeera, al. 2023. "Israeli Military Uses Drones to Kill Palestinians in West Bank's Tulkarem". Aljazeera.Com, December 17, 2023. https://www.aljazeera.com/news/2023/12/17/israeli-military-uses-drones-to-kill-palestinians-in-west-banks-tulkarem.

[38] Sophia Goodfriend. 2023. "Drones Terrorized Gaza for Years. Now They'll Do the Same in the West Bank". +972 Magazine. October 13, 2023. https://www.972mag.com/drones-idf-west-bank-gaza.

[39] By Reuters, and Toi Staff. 2024. "Jordan Thwarts Iran-Led Plan to Carry out Acts of Sabotage in Kingdom – Sources". The Times of Israel, May 15, 2024. https://www.timesofisrael.com/jordan-thwarts-iran-led-plan-to-carry-out-acts-of-sabotage-in-kingdom-sources; Also in Paola Testa. 2024. "CLASSIFIED 1948/2024: What Israeli AI Implementation Teaches Us About the Warfare of Tomorrow". Global Network of Extremism & Technology. March 18, 2024. https://gnet-research.org/2024/03/18/classified-1948-2024-what-israeli-ai-implementation-teaches-us-about-the-warfare-of-tomorrow.

[40] AP. 2024. "Iran Says It Gave Hamas Rocket Technology". The Times of Israel, August 4, 2024. https://www.timesofisrael.com/iran-says-it-gave-hamas-rocket-technology.

[41] Open Source Intel in X. 2024. "Iran's Plot to Arm Judea and Sameria Terrorists Foiled by Shin Bet". X . X. https://x.com/Osint613/status/1861742609107935363?referrer=grok-com.

[42] Jazeera, al. 2024. "Deadly Israeli Raids in Occupied West Bank as Gaza War Rages". Aljazeera.Com , August 29, 2024. https://www.aljazeera.com/gallery/2024/8/29/deadly-israeli-raids-in-occupied-west-bank-as-gaza-war-rages; Also in Zena Al Tahhan. 2023. "West Bank Fighters Say Israel War on Gaza Inspires More Resistance". Al Jazeera , December 12, 2023. https://www.aljazeera.com/features/2023/12/12/west-bank-fighters-say-israel-war-on-gaza-inspires-more-resistance.

[43] Or Yissachar, and Yossi Kuperwasser. 2023. "Israel Security Briefing #6 – H2 June 2023: Rising Palestinian Terrorism In Judea and Samaria". Israeli Defense and Security Forum. July 4, 2023. https://idsf.org.il/en/papers/israel-security-briefing-6-h2-june-2023-rising-palestinian-terrorism-in-judea-and-samaria; Also in Open Source Intel in X. 2023. "Weapons Seized in Shin Bet and IDF Operation Foiling Iran's Smuggling to Judea and Samaria". X . X. https://x.com/Osint613/status/1861809237929624021?referrer=grok-com.

### 4.2.2 Rockets and Anti-Tank Weapons

Smuggling efforts by Iran to introduce RPG launchers and rockets, including RPG-7 launchers with PG-7V/M rockets, single-use RPG-18 and RPG22 rockets, and tandem rockets such as the "Al-Yassin 105." North Korean F-7 rockets and variants of Iranian tandem missiles have also been documented in use by terrorist and guerrilla cells operating in Judea and Samaria.[44] Sixty-millimeter mortar systems, including Iranian M61 shells, are used for indirect fire. Israeli tactical operational activity uncovered two mortar tubes and twenty rounds.[45]

### 4.2.3 Small Arms

The terrorists use a range of assault rifles, machine guns, and rifles, including Hungarian 65-AMD assault rifles; Chinese 56-1 and 80-type machine guns; Libyan-sourced 103-AK model rifles; Yugoslavian M70B1s; and captured Israeli M16/M4 variants seized in the field.

Locally produced sniper rifles such as the Al-Ghul (modeled on the Austrian Steyr HS .50, caliber 12.7 mm) represent a significant technological achievement. They can be converted from assault to sniper configuration and can use custom ammunition: training rounds, incendiary rounds for flammable targets, armor and helmet-piercing rounds, ceramic vests and fortifications at ranges up to 1,800 meters. Other sniper rifles include captured Hunter models (seven such rifles have been seized) and SVD Dragunov variants.[46] Special units of guerrilla fighters in Judea and Samaria train for a durable combat and prolonged field operations.[47]

## 4.3 Advanced Combat Methods in Syria

Rebel operations in Syria, and later the fighting in the urban area of Sweida, make it possible to examine the weapons systems used. Fighters in Syria employ advanced methods of warfare that mark a transition from light weapons and traditional artillery to more sophisticated systems such as drones, remotely operated systems, and advanced optics. This reflects broader trends in the Syrian conflicts, in which inexpensive and readily available technology—such as modified commercial drones—is adapted for combat.[48] Below is a review of this subject.

---

[44] War Noir in X. 2025. " 'Al-Qassam Brigades' (#HAMAS) Carried out Multiple Attacks against #IDF Troops and Merkava Tanks in #Gaza". X . X. https://x.com/war_noir/status/1956449715710550088?referrer=grok-com.
[45] War Noir in X. 2025. " 'Al-Quds Brigades' Released a New Video of Group's Fighters in Eastern #Gaza". X . X. https://x.com/war_noir/status/1957020183547003130?referrer=grok-com.
[46] Open Source Intel in X. 2023. "Weapons Seized in Shin Bet and IDF Operation Foiling Iran's Smuggling to Judea and Samaria". X . X.https://x.com/Osint613/status/1861809237929624021?referrer=grok-com.
[47] Arya - آری in X. 2024. "Al-Qassam Produced the Appropriate Ammunition to Enhance the Rifle's Effectiveness and Feasibility". X . X.https://x.com/AryJeay/status/1769463496356348100?referrer=grok-com.
[48] Nidal Morrison, Avery Borens, and Et.Al. 2025. "Iran Update". https://www.understandingwar.org/backgrounder/iran-update-august-20-2025.

### 4.3.1 Armed Drones and Unmanned Aerial Vehicles

Ethnic Druze militias, Bedouin fighters and opposition gunmen all used modified commercial drones, such as DJI Mavic models equipped with grenades or explosives for precision attacks. For example, Druze fighters were documented dropping grenades from drones onto gunmen affiliated with the Syrian government or with ISIS who were advancing in Sweida.[49]

On the other side, fighters of Hay'at Tahrir al-Sham (HTS) carried out attacks using drones armed with 30 mm VOG-17 grenades launched from the air against Druze positions; one such drone (labeled Abu Anas al-Shami) was shot down during an attack on the town of Shahba.[50] Drones were part of broader bombardments that also included mortars, artillery, and Grad rockets, and they contributed to siege-like conditions in the city.[51]

**Remote-Controlled Weapon Systems (RCWS)**

Druze militias deployed heavy machine guns operated remotely, such as systems mounting 12.7 mm DSHKM or W-85 HMG machine guns, allowing operators to engage targets from protected positions while minimizing exposure. Video footage shows Druze fighters using these systems to fire on HTS cells in Sweida—often in relaxed settings, while smoking or resting.[52]

### 4.3.2 Night-Vision and Thermal-Imaging Equipment

Syrian special-forces units affiliated with HTS, including formations such as the Red Bands, were equipped with thermal-imaging scopes and night-vision goggles for operations west of Sweida City. These tools enable effective night ambushes and surveillance and provide an advantage under low-visibility conditions during the ongoing siege.[53]

### 4.3.3 Satellite Communication (Starlink) and other Advanced Support

Attacking Bedouin forces and HTS units have used Starlink terminals to provide reliable and resilient internet and communications service, which facilitated coordination in areas where local infrastructure—electricity, telephone, communications, and internet—had been cut by Damascus authorities. This technology supported their drone operations and their deployment of forces against Druze resistance.[54]

---

[49] Metatron in X. 2025. "Druze Drone Drops a Grenade on Syrian Government ISIS Militants Attacking #Suwayda". X . X. https://x.com/Narreddine/status/1952071950798385503?referrer=grok-com.

[50] War Noir in X. 2025. "'Hay'at Tahrir al-Sham' (#HTS) Members Are Attacking #Druze Positions with Armed Drones in #Suwayda". X . X. https://x.com/war_noir/status/1946256035884220782?referrer=grok-com.

[51] Karim Franceschi in X. 2025. "They Had Drones, Starlink". X . X. https://x.com/karimfranceschi/status/1947232878946906296?referrer=grok-com.

[52] War Noir in X. 2025. "Druze Militias Operating a Remote-Controlled Machine Gun While Chilling in #Sweida". X . X. https://x.com/war_noir/status/1957136725433622980?referrer=grok-com.

[53] Woofers in X. 2025. "Syrian Special Forces Equipped with Thermal Imaging Scope and Night Vision Equipment Are Now Present West of Suwayda City. Allegedly Members of HTS's Red Bands Unit". X . X. https://x.com/NotWoofers/status/1945197328496726121?referrer=grok-com.

[54] Karim Franceschi in X. 2025. "They Had Drones, Starlink". X . X. https://x.com/karimfranceschi/status/1947232878946906296?referrer=grok-com

In addition, precision-guided munitions such as French wire-guided SS.11 anti-tank missiles (from the 1950s but still effective) were discovered in Druze-militia stockpiles after the clashes, indicating access to previous generation weapons technology.[55]

## 4.4 Hezbollah

Hezbollah employs a combination of advanced-warfare methods and technologies alongside so-called "low-tech" systems. Although it is often portrayed as relying on guerrilla and asymmetric tactics, many of Hezbollah's technological methods originate in Iran.[56] Here too, our review is not limited to Hezbollah's activity in the urban arena, yet it sheds light on the organization's modes of operation in that arena and offers lessons applicable to other theaters, such as Judea and Samaria.

### 4.4.1 Drones and Unmanned Aerial Systems (UAS)

Hezbollah has extensively deployed drones for reconnaissance, attack, and intelligence gathering. These include strike and surveillance drones of models supplied by Iran, such as the Shahed-136, which the organization used in attacks against Israeli targets, often in combination with missiles for coordinated strikes.[57] Use of drones with fiber-optic guidance has also been identified. These systems cannot be detected by radar and are resistant to electronic jamming. Such drones were used in the Russia–Ukraine war and have enabled Hezbollah to bypass Israel's aerial defense array in order to carry out precision strikes.[58]

Hezbollah also developed counter-drone systems, such as the Mithaq-3 surface-to-air missile system, which in 2025 downed an Israeli Hermes 900 UAV using a jam-resistant thermal-seeking device and a high-explosive warhead (range: 5 km, altitude: 4 km, speed: 600 meters per second).[59]

---

[55] Mohamed ELDoh. 2025. "Syria and Saudi Arabia's Northern Front: A New Theatre for the Kingdom's Security Policy". Global Security Review. June 2025. https://globalsecurityreview.com/syria-and-saudi-arabias-northern-front-a-new-theatre-for-the-kingdoms-security-policy; Also in Warfare Analysis in X. 2025. "After Expelling the Israeli-Backed Hijri Druze Militia, Bedouin Forces in Suwayda Discovered a Weapons Depot Including French SS.11 Wire-Guided Anti-Tank Missiles, Developed in the 1950s and Used by Many Countries, Including Israel". X . X. https://x.com/warfareanalysis/status/1946623688784171518?referrer=grok-com.

[56] Nagi N.Najjar in X. 2025. "Hezbollah Upgrading Its ATGM Arsenal in Southern Lebanon LB, Triple Guided Anti Tank Launcher Made in Iran IR (Dehlavieh, Copy of the Russian RU ATGM Kornet)". X. X. https://x.com/NagiNajjar/status/1957181784527138865?referrer=grok-com; Also in Royal Intel in X. 2025. "Hezbollah Is Putting the Majority of Its Efforts into Developing More Advanced Electronic Warfare Due to the Technological Advances That the Enemy Has on the Resistance, 80% of the Enemy's Capabilities Are Electronic". X . X. https://x.com/RoyalIntel_/status/1892734168397652290?referrer=grok-com.

[57] Current Report in X. 2024. "Hezbollah Has Been Using Some Low-Tech Strategies to Try to Evade Israel's Sophisticated Surveillance Technology". X . X. https://x.com/Currentreport1/status/1810937437167964622?referrer=grok-com.

[58] Emily Schrader - אמילי שריידר اميلى شريدر in X. 2024. "Breaking: Hezbollah Apparently Used Fiber-Optic Drones, a Technology Primarily Employed by Russia in Ukraine". X . X. https://x.com/emilykschrader/status/1845535110654795971?referrer=grok-com.

[59] EllenJAbare in X. 2025. "Hezbollah Downing a Hormuz 900 Drone Using the Mithaq-3 System". X . X. https://x.com/EllenAbare/status/1957318340000526774?referrer=grok-com.

### 4.4.2 Precision Missiles and Anti-Tank Guided Missiles (ATGM)

The organization has used advanced rockets and missiles, including Iranian replicas such as the Dehlavieh—based on Russian Kornet missiles—often in barrages coordinated with drone strikes.[60] Short-range systems and anti-tank systems deployed south of the Litani River included guided missiles aimed at Israeli armored vehicles and infrastructure. Before Israel's strike, Hezbollah's stockpile was estimated to include tens of thousands of such weapons.[61]

### 4.4.3 Electronic and Cyber Warfare

Hezbollah has invested in countering Israel's technological dominance through the development of electronic warfare, giving priority to advanced electronic systems designed to disrupt Israeli surveillance.[62] The organization has conducted limited cyberattacks targeting Israeli network, often through Iranian agents.[63] Hezbollah has also been observed participating in Iranian cyber efforts against Israel.

The organization attempted to revert to low-technology tools in order to evade advanced surveillance systems—for example, by returning to the use of pagers and human couriers. Operations such as the booby-trapped pager attack in 2024 highlighted the vulnerabilities of the guerrilla organization.[64]

## 4.5 ISIS in Syria, Iraq, and the Sinai Peninsula

ISIS's technological operations in Syria, Iraq, and the Sinai Peninsula includes drones and precision guided weapons. These technologies, combined with tactical flexibility, allowed ISIS to achieve military successes despite suffering defeat at the hands of coalition forces. In Syria and Iraq, their actions were enabled by access to captured heavy weapons and to drones, while ISIS in the Sinai Peninsula (*Wilayat Sinai*) relied more on guerrilla tactics and explosive devices because of resource constraints. ISIS fighters used a variety of advanced methods in their combat tactics. Below is an analysis of the organization's use of advanced technologies and tactics.

---

[60] Nagi N.Najjar in X. 2025. "Hezbollah Upgrading Its ATGM Arsenal in Southern Lebanon LB, Triple Guided Anti Tank Launcher Made in Iran IR (Dehlavieh, Copy of the Russian RU ATGM Kornet)". X . X. https://x.com/NagiNajjar/status/1957181784527138865?referrer=grok-com.
[61] AJC American Jewish Committee. 2024. "What to Know About Hezbollah's Escalation Against Israel". October 26, 2024. https://www.ajc.org/news/what-to-know-about-hezbollahs-escalation-against-israel.
[62] Royal Intel in X. 2025. "Hezbollah Is Putting the Majority of Its Efforts into Developing More Advanced Electronic Warfare Due to the Technological Advances That the Enemy Has on the Resistance, 80% of the Enemy's Capabilities Are Electronic". X . X. https://x.com/RoyalIntel_/status/1892734168397652290?referrer=grok-com.
[63] Amal Chmouny. 2025. "The Impact of Israeli Cyber Operations on Hezbollah". Arab Center Washington DC , April. https://arabcenterdc.org/resource/the-impact-of-israeli-cyber-operations-on-hezbollah; Also in Bilal Y. Saab. 2025. "Why Hezbollah Fell". Georgetown Journal of International Affairs , March. https://gjia.georgetown.edu/2025/03/31/why-hezbollah-fell; Also in The Sunday Times. 2025. "Unit 8200: Cyber Spies, Psyops & Occult Magic". The Sunday Times , June 31, 2025. https://thesudantimes.com/international/unit-8200-cyber-spies-psyops-occult-magick.
[64] Justin Salhani. 2024. "Exploding Pagers, Psychological Warfare: Israel's Attack on Hezbollah". Al Jazeera , September 18, 2024. https://www.aljazeera.com/news/2024/9/18/chk_exploding-pagers-psychological-warfare-israels-attack-on-hezbollah.

### 4.5.1 Drones and Unmanned Aerial Vehicles

ISIS increasingly used commercially available drones, such as DJI Phantom models, for both reconnaissance and offensive operations. In Syria and Iraq these drones were adapted for combat and were often equipped with landing mechanisms to deliver explosives. By 2025, posts on X indicated that ISIS in Syria still used basic commercial drones such as the Phantom, while more advanced FPV (first-person-view) drones have appeared in other areas—such as Africa—suggesting the potential for capability upgrades.

Drones enabled ISIS to conduct surveillance, identify targets, and carry out precision strikes with minimal risk to its fighters. In urban battlefields such as Mosul, drones provided real-time intelligence and enabled coordinated strikes. Their low cost and accessibility turned them into a force multiplier for guerrilla groups that lack conventional airpower. In the Sinai Peninsula, Wilayat Sinai used drones as well, although less extensively because of resource constraints. Their drone operations were mainly for reconnaissance and to support larger attacks on Egyptian forces.[65]

### 4.5.2 Precision-Strike Technologies

ISIS acquired advanced weaponry, including missiles and anti-tank weapons, among them the Turkish-made 66-HAR, which was observed in use by ISIS fighters in Syria through August 2025.[66] In the Sinai Peninsula, Wilayat Sinai used precision strike methods in coordinated attacks—for example, the assault on 15 security checkpoints at Sheikh Zuweid in 2015—demonstrating its ability to employ advanced weapons that were either captured or smuggled into the peninsula in complex operations.[67]

These precision-strike capabilities were employed in large-scale operations with sustained persistence aimed at seizing and controlling territory, as seen in ISIS's territorial gains in Iraq and Syria between 2014 and 2017. Between 2011 and 2014 ISIS looted military bases and captured materiel from Iraqi and Syrian forces. Among other items, it obtained large quantities of military equipment, including U.S. M1 Abrams tanks, Soviet-era T-55 and T-72 tanks, and artillery systems. These weapons enabled the group to conduct sustained fighting during its rapid territorial gains and expansion in 2014, such as the capture of Mosul.[68]

[65] Khalil Al-Anani. 2022. "Insurgency in Sinai: Challenges and Prospects". Arab Center Washington DC , June. https://arabcenterdc.org/resource/insurgency-in-sinai-challenges-and-prospects.
[66] Khalil Al-Anani. 2022. "Insurgency in Sinai: Challenges and Prospects". Arab Center Washington DC , June. https://arabcenterdc.org/resource/insurgency-in-sinai-challenges-and-prospects.
67 Mutschler, Max, Marius Bales, and Esther Meininghaus. 2024. "The Impact of Precision Strike Technology on the Warfare of Non-State Armed Groups: Case Studies on Daesh and the Houthis". Small Wars & Insurgencies 35 (7): 1123–50. doi:10.1080/09592318.2024.2319216
[68] European Institute of Peace. n.d. "Tyranny of Evil. The Legacy of ISIS in Northern Syria". Accessed August 24, 2025. https://www.eip.org/report-on-the-legacy-of-isis-rule-in-northeast-syria/military-tactics; Also in Cenkay Uyan, and Omar Ashour. 2023. "How ISIS Fights?: Military Tactics in Iraq, Syria, Libya, and Egypt". INSIGHT Turkey. 2023.

UN Security Council report in 2014 noted that ISIS possessed man-portable air-defense systems (MANPADS) such as the SA-7, which posed a threat to low-altitude aircraft and helicopters. This was particularly relevant in Iraq and Syria, where coalition airstrikes proved a major challenge for ISIS cells.[69]

### 4.5.3 Improvised Explosive Devices and Vehicle-Borne IEDs

ISIS developed the capability to design and manufacture improvised and sophisticated explosive devices, often using advanced improvised firing mechanisms such as pressure-plate devices and systems enabling remote detonation. In Iraq—especially during the Battle of Mosul between 2016 and 2017—ISIS deployed vehicle-borne IEDs (VBIEDs) at a rate of 10–15 per day, with nearly 80% success, causing significant disruption to the anti-terrorist operations of Iraqi forces.[70]

In Sinai, the Wilayat Sinai terrorist group carried out 134 explosive-charge attacks in 2019 alone, demonstrating its reliance on this technology to strike Egyptian military and civilian infrastructure. These attacks were often coordinated with complex strikes on fortified positions of Egyptian security forces and demonstrated tactical sophistication.[71]

### 4.5.4 Cyber Activity and Communications

ISIS's *al-Hayat* media center played a central role in leveraging advanced media tools to produce polished propaganda, videos and online content that were distributed via platforms such as Telegram and Twitter. This was critical for recruiting fighters, inspiring lone-actor attacks around the world, and maintaining morale among fighters in Syria, Iraq, and the Sinai.[72]

ISIS used basic cyber tools for communications, coordination, and occasional intrusion attempts intended to disrupt opponents' operations. Its strong and permanent presence online enabled the dissemination of tactical knowledge among its members—for instance, bomb-making guides and instructions. Wilayat Sinai used social networks to claim responsibility for attacks, such as the 2017 mosque attack in Bir al-Abd, which killed 311 people, thereby amplifying the organizations psychological impact among supporters regionally and globally.[73,74]

[69] European Institute of Peace. n.d. "Tyranny of Evil. The Legacy of ISIS in Northern Syria". Accessed August 24, 2025. https://www.eip.org/report-on-the-legacy-of-isis-rule-in-northeast-syria/military-tactics.
[70] Becca Wasser, Stacie L. Pettyjohn, and Et Al. 2021. "The Role of U.S. Airpower in Defeating ISIS". RAND , February. https://www.rand.org/pubs/research_briefs/RBA388-1.html.
[71] US Department of State. 2019. "Country Reports on Terrorism 2019". https://www.state.gov/reports/country-reports-on-terrorism-2019.
[72] Mapping Militant Organizations. "Islamic State". Last modified April 1, 2021. https://mappingmilitants.org/node/407.
[73] Tønnessen, Truls Hallberg. "Islamic State and Technology – A Literature Review". Perspectives on Terrorism 11, no. 6 (2017): 101–11. http://www.jstor.org/stable/26295959.
[74] David E. Thaler, and Yousuf Abdelfatah. 2019. "Making Headway Against the Sinai Insurgency". RAND , August. https://www.rand.org/pubs/commentary/2019/08/making-headway-against-the-sinai-insurgency.html.

## 4.6 Latin America

Guerrilla warfare in South America has evolved significantly through the integration of technology and is driven by both state and nonstate actors adapting to modern challenges. While traditional guerrilla tactics relied on mobility, surprise, knowledge of localities, and familiarity with the terrain, in recent decades groups such as the FARC in Colombia and criminal organizations in Brazil have incorporated advanced tools to enhance their operations.

### 4.6.1 The Use of Drones and Unmanned Aerial Vehicles

The use of drones and unmanned aerial vehicles by guerrilla fighters in Latin America is especially widespread. In Colombia, the National Liberation Army (ELN) used camera-guided drones with infrared capability to drop grenades on Colombian soldiers—demonstrating how even jungle guerrillas have adopted modern aerial technology. A 2025 incident report highlighted the growing accessibility of such systems in remote areas. In Brazil, in Rio de Janeiro, the Terceiro Comando Puro (TCP) attacked its rival, the Comando Vermelho (CV), using DJI Mavic 3 drones equipped with improvised Mk 2 fragmentation grenades. This illustrates how criminal groups, which often use guerrilla tactics, leverage commercial drones for urban warfare. Across South America, both militaries and guerrillas use UAVs for intelligence, surveillance, reconnaissance, and combat. Countries in Latin America have developed their own drone systems such as Argentina (Lipán M3), Brazil (VT-15s), and Colombia (Navigator X2, Iris)—some with facial-recognition capabilities—though these remain in the hands of state bodies, primarily security forces. Many guerrilla groups, however, adapt commercial drones for similar purposes.[75]

### 4.6.2 Communication Technologies

The Revolutionary Armed Forces of Colombia (FARC) traditionally relied on radio-based communications, which, while serving as a critical infrastructure for the group, was highly vulnerable. The Colombian army's introduction of surveillance and localization technologies (signal tracking and interception) posed a lethal threat and forced the FARC to adopt technical countermeasures and more secure communication protocols. This serves as an example of a "counter-appropriation" process, in which guerrilla fighters adapt to technological advances and the improved surveillance capabilities of state security forces.[76]

[75] Frank O. Mora, Brian Fonseca. 2015. "Latin America's High-Tech Warriors". Americas Quarterly , May 7, 2015. https://www.americasquarterly.org/fulltextarticle/latin-americas-high-tech-warriors.
[76] Débora de Castro L., M. Krüger, K. Misaki, D. Randall, and V. Wulf. 2019. Guerilla Warfare and the Use of New (and Some Old) Technology: Lessons from FARC's Armed Struggle in Colombia. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 580, 1–12. https://doi.org/10.1145/3290605.3300810.

## 4.7 Southeastern Ukraine

The war and separatist insurgency in southeastern Ukraine constitute an important case study for examining both modern hybrid warfare and urban guerrilla warfare. The use of technology by separatist forces in southeastern Ukraine—particularly in the Donbas region (the Donetsk and Luhansk republics)—has been significant since the outbreak of the conflict in 2014. These forces, supported by Russia, have leveraged a variety of technologies to conduct hybrid warfare that combines conventional military tactics with technological tools.

The separatist forces rely heavily on Russian support for advanced technologies, which limits their autonomy and operational freedom. Russian technological countermeasures, such as electronic-warfare systems, are not always applied uniformly or correctly, resulting in accidents, damage, and the destruction of valuable equipment—and even its capture by the enemy.[77]

Ukrainian forces have rapidly adapted to this new reality, employing their own drones, electronic-warfare systems, and artificial-intelligence–based technologies to counter separatist capabilities. For example, the Ukrainian military's "Spider Web" operation, in which a swarm of drones was sent into Russian territory and destroyed strategic transport aircraft, demonstrated the effectiveness of low-cost FPV drones against high-value Russian targets and exposed vulnerabilities and failures in Russian air defenses.[78]

The separatists' use of technology in southeastern Ukraine reflects a broader trend in modern irregular warfare—a "democratization" of weaponry, and the ease of access to advanced tools such as drones, electronic weapons, and cyber capabilities. These technologies, often supplied by Russia, enable relatively small forces to challenge the Ukrainian army. However, the effectiveness of these technologies depends on their integration with Russian support, training, and logistics. In other words, the effectiveness of hybrid separatist warfare depends on state sponsorship—forcing both sides into a cycle of armament and counter-innovation.[79]

### 4.7.1 Drones and Unmanned Aerial Vehicles

Unmanned aerial vehicles (UAVs/drones) are used extensively by the pro-Russian separatist forces. Most systems are supplied by Russia itself; however, at present the

[77] Gregory C. Allen, Kateryna Bondar, Samuel Bendett. 2025. "The Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond". https://www.csis.org/analysis/russia-ukraine-drone-war-innovation-frontlines-and-beyond.
[78] Kateryna Bondar. 2025. "How Ukraine's Operation 'Spider's Web' Redefines Asymmetric Warfare". https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare.
[79] Gregory C. Allen, Kateryna Bondar, Samuel Bendett. 2025. "The Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond". https://www.csis.org/analysis/russia-ukraine-drone-war-innovation-frontlines-and-beyond; Also in Kateryna Bondar. 2024. "Understanding the Military AI Ecosystem of Ukraine". https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine

pro-Russian separatists also employ, in some cases, independently produced UAVs. Their primary use of drones is for intelligence, surveillance, and reconnaissance (ISR), as well as for direct attacks. Commercial drones—including modified variants—were already used for ISR missions as early as 2014. By 2016 the separatists had begun adapting commercial drones to drop grenades on Ukrainian positions.

Military-grade drones supplied by Russia, such as the Orlan-10, were deployed for advanced reconnaissance and to guide precision strikes. Drones provide the separatist forces with a low-cost, high-impact tool that expands their operational range, compensating for manpower and conventional limitations. Their use became a hallmark of the technological "evolution" of the Russian—Ukrainian conflict. The separatists, with Russian backing, have also used electronic-warfare systems to disrupt Ukrainian communications, GPS signals, and drone operations by government security forces. These systems jam or spoof signals, making Ukrainian drones and communication networks less effective.

### 4.7.2 Electronic Warfare

Advanced weapons systems operated by irregular separatist guerrilla organizations represent a new trend in modern asymmetric warfare. For example, several Russian electronic-warfare systems, such as the Borisoglebsk-2, were struck by Ukrainian forces during fighting against separatists in southeastern Ukraine, suggesting that these systems were used by pro-Russian separatists, Russian military experts on site or by Russian proxies.[80] Mobile and vehicle-mounted electronic-warfare systems were deployed to counter Ukrainian drones, particularly single-operator FPV drones. These systems enhance the defense and offensive capabilities of the separatists by neutralizing Ukrainian technological advantages, especially in drone warfare. However, Russian electronic-warfare systems, though advanced, face reliability challenges and system integration problems that limit their overall effectiveness.[81]

### 4.7.3 Cyber and Cognitive Warfare

Cyberwarfare, cognitive-influence and propaganda operations have also been employed. Ukrainian separatist forces, supported by Russian intelligence, participated in cyber operations aimed at disrupting Ukrainian infrastructure and spreading disinformation. These efforts align with Russia's broader information-warfare strategy and psychological warfare, designed to undermine governmental stability in Ukraine and shape narratives among the local population. Cyber operations by separatist actors, assisted by Russian

[80] Daniel Sullivan, Riley Murray, Rylan Neely. 2025. "Lessons from the Frontlines: Ukrainian SEAD Operations and Their Implications for Western Special Operations Forces". Irregular Warfare Initiative , February. https://irregularwarfare.org/articles/ukrainian-sead-operations-lessons-for-western-sof.
[81] Daniel Sullivan, Riley Murray, Rylan Neely. 2025. "Lessons from the Frontlines: Ukrainian SEAD Operations and Their Implications for Western Special Operations Forces". Irregular Warfare Initiative , February. https://irregularwarfare.org/articles/ukrainian-sead-operations-lessons-for-western-sof.

forces, included distributed denial-of-service (DDoS) attacks and the use of malware such as FoxBlade, intended to penetrate and damage Ukrainian command-and-control systems.[82]

Disinformation campaigns, information and public opinion manipulation, and perception-shaping operations directed at ethnic Russians in eastern Ukraine were used to incite separatist rebellion and justify Russian intervention.[83] These activities—combining propaganda, cyberwarfare, misinformation, and perception management—strengthen separatist efforts by sowing confusion, undermining Ukrainian governance, and mobilizing local support. Such operations are often coordinated with Russian special-forces activities.

### 4.7.4 Precision-Guided Weapons and Drone-Based Fire Support

The separatist forces relied on precision-guided munitions and artillery systems supplied by Russia, often coordinated through drones or electronic technologies to enhance their firepower and accuracy. Russian artillery support, including systems such as the BM-21 Grad, was operated in cooperation with separatist units to strike Ukrainian positions with high precision, guided by reconnaissance and intelligence gathered by drones. Pro-Russian separatists were trained by Russian special-forces units (Spetsnaz) to operate weapons systems integrated with advanced technologies, improving their effectiveness in combined operations.[84]

### 4.7.5 Communications and Command

Pro-Russian separatists employ communications systems supplied by Russia to maintain command and control, often in environments where Ukrainian forces seek to disrupt them. For example, Russian commercial satellite systems and their military equivalents have been used to maintain communication with drones and special units in the field when ground-based networks are disrupted by Ukrainian jamming efforts and cyberattacks.[85]

In addition, technologies such as mesh networks and portable routers (satellite or airborne relays) allow separatist units to operate despite Ukrainian electronic warfare interference.[86] Robust communications systems ensuring coordination between separatist units and Russian operational coordinators in the field constitute a critical component of

[82] Tech Informed. 2023. "One Year on: 10 Technologies Used in the War in Ukraine". Tech Informed. February 24, 2023. https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine.
[83] The United States Army Special Operations Command. 2025. "Little Green Men: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014". Fort Bragg, North Carolina. https://nsarchive.gwu.edu/document/16170-us-army-special-operations-command-little-green.
[84] Bret Perry. 2015. "Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations". Small Wars Journal, August. https://archive.smallwarsjournal.com/index.php/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera.
[85] Matthew Slusher. 2025. "Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience". https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience.
[86] Matthew Slusher. 2025. "Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience". https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience.

sustaining irregular warfare in the hybrid and dynamic battle environment.

Russian Spetsnaz special forces units, including units belonging to the GRU (military intelligence), have played a central role in training and advising separatist forces. Training focuses on small-scale, unconventional warfare, including tactical training to outmaneuver Ukrainian command centers and concentrations of forces. For example, the Vostok Battalion, which began as a locally supported separatist force backed by Russia, has evolved into a well-trained guerrilla formation under Russian instruction.[87]

The building and integration of proxy forces into irregular hybrid warfare became a decisive element in the war between Russia and Ukraine. The militias of the Donetsk and Luhansk People's Republics were formally incorporated into Russia's regular armed forces. In other words, one of the warring states achieved extensive military deployment on enemy territory "without leaving home." Formally, separatist guerrilla forces in southeastern Ukraine began receiving assistance from the Southern Command headquarters of Russia's Southern Military District as early as February 2022, gaining direct support in weaponry, technology, supplies, and logistics.[88] Prior to that point, Russian support had been largely covert and deniable.

### 4.7.6 Sniper Operations

According to reports, a Ukrainian sniper operating on the front line in Ukraine set a new world record for the longest-ever sniper shot. The long-range hit was achieved with the aid of artificial intelligence and struck two Russian soldiers simultaneously. A Telegram post accompanied by a video of the shot reported that a sniper using a Ukrainian-made Snipex Alligator rifle hit his target at a distance of 4,000 meters. It was also revealed that the shot was assisted by a precision system based on artificial intelligence. The AI system made firing adjustments from an unmanned aerial vehicle hovering over the target area.[89]

### 4.7.7 Private Contractors

The phenomenon of private military companies (PMCs) has been implemented extensively in the Russian—Ukrainian conflict. Companies such as Wagner,[90] Tsar Wolves,[91] and Redut[92]

[87] Perry. 2015. "Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations". Small Wars Journal, August. https://archive.smallwarsjournal.com/index.php/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera.
[88] FOX NEWS. 2014. "US: Separatists in Eastern Ukraine Have Weapons, Military Equipment from Russia". June 13, 2014. https://www.foxnews.com/world/us-separatists-in-eastern-ukraine-have-weapons-military-equipment-from-russia.
[89] thedailydigest.com. 2025. "Record Breaking Success: Ukrainian Sniper Fires Longest Kill Shot Ever". Msn.Com. August 14, 2025.
[90] Brian Latham. 2023. "Wagner Isn't the Only Proxy Company Waging the Kremlin's Widening World War – It's Just the Biggest". ByLine Times. May 4, 2023. https://bylinetimes.com/2023/05/04/wagner-isnt-the-only-proxy-company-waging-the-kremlins-widening-world-war-its-just-the-biggest.
[91] Azerbaycan 24. 2022. "Former Russian Space Boss Leads 'Tsar Wolves' in Donbass". Azerbaycan 24. November 11, 2022. https://www.azerbaycan24.com/en/former-russian-space-boss-leads-tsar-wolves-in-donbass.
[92] Tor Bukkvolla, Åse G. Østensen. 2020. "The Emergence of Russian Private Military Companies: A New Tool of Clandestine Warfare". Kjeller, Bergen, Norway. https://doi.org/10.1080/23296151.2020.1740528.

served as auxiliary and complementary forces supporting the separatists with manpower, logistical assistance, advanced technology, and expertise. The use of PMCs also has a technological dimension. Russia used its war against Ukraine as a testing ground for its new technologies and weapons systems. For example, Tsar Wolves cooperated with Russia's defense industry to test new technologies in the fighting in southeastern Ukraine (Donbas).

## 5. Emerging Modes of Combat

Future technological innovations in guerrilla warfare are likely to build on current trends, in which terrorist groups, nonstate actors, or smaller forces leverage affordable, adaptable technology to contest superior conventional militaries. The review below emphasizes emerging modes of combat in Judea and Samaria (and possibly in Gaza) and offers a general account of developments expected in the near term. It should be read in conjunction with the case studies described above.

### 5.1 Drones and Autonomous Systems

Drones are likely to become central to hybrid operations, and their use will expand beyond surveillance, to swarms intended to saturate or overwhelm systems of opposing forces, as well as to conduct precision strikes and electronic disruption— especially against the IDF in Judea and Samaria and even in Gaza. Groups such as the Houthis have already demonstrated this by using smuggled drone components reassembled in the field for long-range operations and sabotage against shipping and critical infrastructure.[93] Future operations may include AI-driven swarms coordinated in real time, complicating defenses such as the Iron Dome through saturation and evasive tactics. Iran is likely to attempt to smuggle such advanced technologies into the Judea and Samaria arena.

In an urban environment, FPV (first-person-view) drones armed with explosives could strike settlements, IDF camps, vehicles, and fighters—as has been observed in Syria where opposition groups such as HTS employed them against regime forces.[94] The concept or tactic of a "battle mesh"—integrative networks that link combat unmanned aerial vehicles (UCAVs) with loitering munitions and electronic-warfare payloads—could emerge among alliances such as Turkey–Azerbaijan–Pakistan, failed states like Syria, rogue states like Afghanistan and para-government entities like the Taliban and impact the way their proxies deploy.

[93] Cameron Hudson in X. 2025. "UAE Is Pioneering a Surrogate Model Where Drones Are Shipped in Parts, Reassembled in the Field". X. X. https://x.com/_hudsonc/status/1932176074995343525?referrer=grok-com.
[94] CALIBRE OBSCURA in X. 2024. "As Long Hinted, Use of HTS FPV Drones with RPG and HE Playloads against SAA Positions and Armour". X . X. https://x.com/CalibreObscura/status/1862027573313569202?referrer=grok-com.

## 5.2 Anti-aircraft Weapons

In Judea and Samaria, Iran can be expected to attempt to infiltrate anti-air and anti-helicopter weapons as part of an ongoing effort to erode the IDF's air superiority in the theater. The threat is more acute when it originates in dense urban terrain that complicates attribution and detection. In the same way that ISIS did in other arenas, Iran can be expected to attempt to introduce mobile air-defense systems and shoulder-fired SAMs capable of threatening low-flying aircraft and helicopters.

## 5.3 Sniper Operations

Although a persistent sniper threat exists against Israeli forces operating in Judea and Samaria, the development of long-range weaponry could pose a materially greater danger. An ambush pattern employing a long-range rifle, such as the Ukrainian Snipex Alligator, within the urban arena could constitute a significant threat to security forces both by day and by night (including through the use of thermal devices). Guidance provided by an AI system and targeting from an unmanned aerial vehicle in the target area could amplify that threat. This tactical pattern does not require sustained action; a single successful strike can markedly disrupt operations.

### 5.3.1 Integration of Artificial Intelligence and Machine Learning

Artificial intelligence can alter guerrilla tactics by enabling predictive analytics for ambush planning, real-time target recognition, and disinformation campaigns.[95] In urban or irregular environments, algorithms may process big data from social networks or from sensor networks to map IDF movements or to optimize "hit-and-run" operations.[96] Gamification elements, such as s augmented-reality overlays for navigation or team coordination, could improve the effectiveness of weapon systems without requiring extensive training.[97]

### 5.3.2 Cyber Tools and Electronic Warfare

Hybrid warfare will increasingly incorporate cyber elements to disrupt communications. Iran-backed groups may shift to cyberwarfare and electronic-warfare tactics aimed at soft targets.[98] AI can enhance these efforts by automating intelligence collection, producing situational analyses for ambushes, or generating deepfakes for disinformation campaigns.

[95] Chris Meserole. 2018. "Wars of None: AI, Big Data, and the Future of Insurgency". LawFare. June 1, 2018. https://www.lawfaremedia.org/article/wars-none-ai-big-data-and-future-insurgency.
[96] Mike Sexton. 2025. "AI and the Evolution of Asymmetric Cyber Warfare: Insights from the 2025 Israel-Iran Conflict". Trend Research & Advisory. August 25, 2025. https://trendsresearch.org/insight/ai-and-the-evolution-of-asymmetric-cyber-warfare-insights-from-the-2025-israel-iran-conflict/?srsltid=AfmBOooCR0KpeOLFPLxtELLlMs0ri5LbEnQOCRh-53KZQ0ldr2DSPmcZ.
[97] Seth G. Jones. 2025. "The Tech Revolution and Irregular Warfare: Leveraging Commercial Innovation for Great Power Competition". Center for Strategic & International Studies CSIS, January. https://www.csis.org/analysis/tech-revolution-and-irregular-warfare-leveraging-commercial-innovation-great-power.
[98] Kasra Aarabi in X. 2025. "With Conventional Military Capabilities Diminished, the Regime Will Pivot to Asymmetric Warfare". X . X. https://x.com/KasraAarabi/status/1940378702006853693?referrer=grok-com.

Future terrorist operations may combine physical attacks with cyber intrusions designed to defeat defensive systems or to disable drones. Digital measures to degrade electronic-warfare capabilities are likely to spread, permitting guerrilla forces to operate across the electromagnetic spectrum and to blind advanced sensors.

Cyber tools may be employed to disrupt communications, to penetrate infrastructure, or to disseminate AI-generated propaganda.[99] Emerging electronic warfare systems could use AI to jam or spoof signals quickly, thereby levelling conditions against a technologically superior adversary.[100]

### 5.3.3 Advanced and Improvised Personal Equipment

Innovations such as powered exoskeletons could enable fighters to carry heavier loads, such as advanced body armor or additional ammunition, while preserving mobility in difficult terrain.[101] Smart optics and augmented-reality goggles could provide night vision, orientation, battlefield positioning, target highlighting, and shared situational awareness, turning lone fighters or lone-actor terrorists into coordinated nodes of a distributed cell[102] composed of a single person. Three-dimensional printing and additive manufacturing could permit on-site production of weapons or custom parts, reducing dependence on supply chains.[103]

### 5.3.4 Integrated Battle Meshes and Hypersonic Fire Capabilities

The "battle mesh" concept—integrated networks of drones, missiles, and sensors—may spread among guerrilla forces through collaboration or open-source tech.[104] Directed-energy weapons (lasers) might appear, although access to such systems by nonstate actors remains uncertain.[105]

Hypersonic weapons would complicate interception and allow strikes on high-value targets with minimal warning and little chance of interception. Broader adoption of solid-fuel missiles and mobile launchers (including light off-road vehicles such as jeeps, pickups, and Hummers) would increase mobility and complicate detection.

[99] Kevin Schaeffer. 2025. "The Future of Conflict Is Now: The Need for Asymmetric Deterrence". Strategy & Insights Hardware. February 25, 2025. https://www.iqt.org/library/the-future-of-conflict-is-now-the-need-for-asymmetric-deterrence.
[100] AI Girl in X. 2025. "Pulsar — Smart Tech for Electronic Warfare (EW) A New Type of System That Fights Using Electromagnetic Signals. Uses AI to Detect and Stop Threats Quickly". X . X. https://x.com/LetsGrowithAI/status/1959602095746855274?referrer=grok-com.
[101] Zhao DaShuai in X. 2024. "Accurate Destruction on Sale in China". X . X. https://x.com/zhao_dashuai/status/1863062852367778006?referrer=grok-com.
[102] Zhao DaShuai in X. 2025. "Gamification of War Is Here". X . X. https://x.com/zhao_dashuai/status/1936797653817532820?referrer=grok-com.
[103] David Kilcullen. 2022. "The End of High-Tech War". March 11, 2022. https://www.technologyreview.com/2020/03/11/905388/the-end-of-high-tech-war.
[104] Amir Husain in X. 2025. "War Has Evolved." X . X. https://x.com/amirhusain_tx/status/1928325162426110143?referrer=grok-com.
[105] Patricia D. Hoffman. 2000. "Seeking Shadows In The Sky: The Strategy Of Air Guerrilla Warfare". https://media.defense.gov/2017/Dec/27/2001861509/-1/-1/0/T_0020_HOFFMAN_SEEKING_SHADOWS_IN_SKY.PDF.

## 6. Summary

This paper examines urban guerrilla warfare with a focus on the arenas of conflict that Israel is expected to encounter, particularly in Judea and Samaria. It highlights how rapid urbanization and technological advancement enable terrorist organizations to exploit simplicity and efficiency against conventional forces, employing methods that destabilize the enemy with minimal resources. Technological revolutions, the end of the Cold War, and global urbanization have all accelerated the use of these methods, by criminal organizations, separatist movements, and terrorist groups alike.

Densely populated urban centers such as Gaza create complex environments that facilitate concealment, mobility, and hit-and-run operations. Technological developments now permit the use of drones for surveillance and attack; of cyberwarfare to disrupt infrastructure; and encrypted communications (WhatsApp, Telegram), alongside 3-D-printed weaponry and AI for planning and analytics. Psychological warfare leverages social networks for recruitment and propaganda, and for sabotage operations including those carried out by lone actors.

Analysis of the phenomenon and its case studies allows for the identification of new modes of warfare and emerging trends. These include the use of autonomous drone swarms, AI-driven predictive analytics, advanced cyber capabilities, specialized personal equipment and exoskeletons, and integrated battle-mesh systems. Such trends will blur the boundaries between regular and irregular warfare and fuel an ongoing arms race within the asymmetric warfare arena.

Urban terrorism and guerrilla warfare have evolved into an adaptive, highly technological form of asymmetric conflict. The convergence of drones, encrypted communication, social media, widespread digitization, and cyber capabilities—together with exploitation of urban terrain and civilian populations—poses major challenges for security forces. Meeting these threats requires a deep understanding of urban environments as the urban arena continues to expand and densify (refugee camps, large villages (Africa, Nigeria, Sudan), West Bank cities and Gaza strip (Israel), ruined cities in failed states, etc.). The complexity of urban warfare will only grow, demanding the development of new and relevant methods of response by Israel's security forces and its allies.

September 2025


**The Jerusalem Institute for Strategy and Security**
16 Abba Eban St, Jerusalem
www.jiss.org.il
info@jiss.org.il

**Conlonel (Res.), Prof. Gabi Siboni** was director of the military and strategic affairs program, and the cyber research program, of the Institute for National Security Studies (INSS) from 2006-2020, where he founded academic journals on these matters. He serves as a senior consultant to the IDF and other Israeli security organizations and the security industry. He holds a B.Sc. and M.Sc. in engineering from Tel Aviv University and a Ph.D. in Geographic Information Systems (GIS) from Ben-Gurion University.

---

**Dr. Simon Tsipis** holds a PhD in political science and international relations from Bonn University and an MA in political science and national security from Tel Aviv University. His areas of expertise include terrorism, cybersecurity, and post-Soviet politics in Eastern Europe and Eurasia.

www.jiss.org.il