Unit 8040 - Iran's Cyber Spearhead in Asymmetric Warfare

Treadstone 71

Unit 8040 is vital to Iran's missile defense and cyber warfare strategy. Led by Ghodratollah Fatemi, it combines air defense with offensive cyber capabilities. Operating from Mosaic Defense locations like Qeshm Island and closely linked to Hezbollah, the unit disrupts enemy defense systems and trains proxy forces. Its actions reflect Iran's focus on asymmetric warfare, blending traditional military power with cutting-edge cyber operations.

Unit 8040, while primarily focused on air defense and missile operations, also holds significant offensive cyber capabilities as part of the broader IRGC cyber operations network. The Islamic Revolutionary Guard Corps (IRGC) has developed a robust cyber warfare capability over the past decade, and Unit 8040, being highly specialized, is likely integrated into these operations. Below is a comprehensive exploration of Unit 8040's offensive capabilities, detailing its methods, areas of expertise, and likely involvement in cyber warfare based on patterns within IRGC operations -

Cyber Warfare Integration

Though primarily engaged in air defense, Unit 8040 is likely part of Iran's offensive cyber efforts, which have rapidly expanded in recent years. Iran has established a sophisticated cyber network through the IRGC, Ministry of Intelligence and Security (MOIS), and Basij Cyber Battalions. These groups often coordinate offensive cyber operations aimed at espionage, sabotage, and propaganda against regional and global targets. Unit 8040's technical background in aerospace and missile systems makes it highly probable that they support offensive cyber operations by -

Securing Iran's missile systems from cyber intrusions - Ensuring the resilience of Iran's critical air defense and missile infrastructure, which enemy cyberattacks could compromise.

Conducting cyber sabotage - Leveraging their expertise in missile technology to support cyber sabotage efforts against enemy missile and defense systems.

Collaborating with Iranian APTs - Using Iranian cyber groups such as APT33, APT34, and APT35 (the Charming Kitten group), Unit 8040 coordinates attacks that disrupt enemy communication, infrastructure, and military operations.

Strategic Cyber Offensives

Iran's cyber strategy often aligns with broader military goals, particularly the asymmetric warfare model that Iran uses to extend its influence. Unit 8040's integration with IRGC cyber operations suggests it might contribute to offensive actions in several key areas -

Disruption of enemy air defense systems - Iran has demonstrated a solid capability to disrupt and infiltrate enemy military infrastructure. Unit 8040, with its air defense focus, could be tasked with conducting cyber operations aimed at disabling or infiltrating enemy air defense networks, such as Israel's Iron Dome system or Saudi Arabia's Patriot missile defense systems.

Cyber Reconnaissance - Advanced Persistent Threat (APT) groups aligned with the IRGC have historically been involved in long-term cyber espionage operations, targeting defense contractors, critical infrastructure, and military networks. Unit 8040's expertise would be invaluable in coordinating real-time intelligence gathered from these cyber intrusions and relaying it to field operations, particularly in regions like Syria, Lebanon, and Iraq.

Preemptive Cyber Strikes - As part of Iran's deterrence strategy, Unit 8040 could be involved in preemptive cyberattacks on adversaries' critical infrastructure to weaken their response capabilities during a military confrontation, attacks on energy grids, communication networks, and transportation systems in enemy countries such as Saudi Arabia, Israel, and the United States.

Key Offensive Capabilities

The offensive capabilities of Unit 8040, linked with the IRGC's cyber apparatus, likely include:

- Advanced Cyber Tools and Malware - Iran has developed a wide range of advanced cyber tools, including custom malware, remote access trojans (RATs), and data-wiping software like *Shamoon* and *StoneDrill*, which have been used in previous attacks on Saudi Arabia and other adversaries. Unit 8040 could use these tools to target enemy infrastructure, especially systems related to air defense and missile technologies.
- Targeted Phishing Campaigns and Social Engineering - Iranian cyber units, including those linked with the IRGC, have been involved in extensive phishing campaigns targeting high-level government officials, military personnel, and defense contractors. Unit 8040 could play a role in orchestrating these attacks, particularly against defense organizations that develop missile defense systems.
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks - Iran has a history of launching DDoS attacks against foreign institutions, particularly financial systems and government websites, as seen in *Operation Ababil*. Unit 8040 could be tasked with launching similar attacks against defense targets to overwhelm communication systems and disrupt military operations during an active conflict.
- Collaborative Offensive Operations with APT Groups - The IRGC's strategy involves outsourcing offensive cyber operations to contractors and academic institutions such as

Shahid Beheshti University and Imam Hossein University, which contribute to developing cyber tools and offensive capabilities. Unit 8040, with its advanced knowledge of missile and air defense systems, would likely collaborate with these entities to refine cyber tools for specific military objectives, such as disabling enemy radar systems or jamming satellite communications.

Missile Guidance and Air Defense Sabotage

Given Unit 8040's specialization in air defense, it is likely involved in cyber operations aimed at disrupting the missile guidance systems of enemy forces. Our findings show they use:

- GPS Spoofing - Iran has developed sophisticated GPS jamming and spoofing capabilities, which have been used to disrupt the guidance systems of unmanned aerial vehicles (UAVs) and enemy missiles. Unit 8040's deep involvement in air defense suggests they could execute similar operations to misguide enemy missiles or UAVs targeting Iranian or proxy forces.
- Hacking Enemy Air Defense Systems - Unit 8040 targets enemy air defense systems, such as Israel's Iron Dome, Saudi Arabia's Patriot systems, or U.S.-based Aegis systems. By gaining access to these systems, they could disable or degrade their ability to intercept incoming missiles, thereby giving Iranian forces or their proxies a strategic advantage during conflicts.

Unit 8040, a specialized entity within Iran's cyber and missile defense strategy, operates under the leadership of Ghodratollah Fatemi, also known as Ghodrat Golabi. Fatemi, identified as the commander of Unit 8040, was born on the 10th of Shahrivar 1355 (corresponding to August 31, 1976), and his national code is publicly known, a rare level of personal detail that suggests a targeted effort to expose his identity. Fatemi's leadership role reflects the increasing importance of Unit 8040 within the IRGC's broader strategy, particularly in air defense and missile technology.

Unit 8040's operations extend beyond traditional missile defense, as the unit has been directly involved in training and deploying air defense systems, specifically the Sevom Khordad, an advanced Iranian surface-to-air missile system. 8040's responsibilities include analyzing, disassembling, and transferring defense technologies to both Iranian forces and Iran's regional proxies. The role of Unit 8040 in these operations highlights its critical function in ensuring that both Iran and its allies, such as Hezbollah, have access to sophisticated defense equipment.

The Shahid Karimi base in Kashan, located adjacent to the Kashan airport, serves as the primary training facility for Unit 8040. Their location underscores the unit's role in

operational defense and in training personnel to use and deploy defense systems. Kashan's strategic importance as a military hub for missile operations and air defense development makes it an ideal location for Unit 8040's activities. Additionally, Garmdarreh has been identified as another site where some of Unit 8040's testing and operational work is conducted, further expanding the geographical scope of the unit's operations.

In recent conflicts, particularly involving Israel and Hezbollah, Unit 8040's involvement has extended into the field. Reports indicate that members of Unit 8040 have been deployed to Lebanon and Syria to provide direct support to Hezbollah. This involvement includes the training of Hezbollah forces and the provision of specialized air defense systems, reinforcing Iran's proxy warfare strategy in the region. The unit's activities in these conflict zones highlight its dual function: defending Iran's missile systems and assisting allied forces in regional power projection.

Beyond military operations, Unit 8040 has played a role in recruitment and logistics for foreign militants trained in Iran. During the recent conflicts, Hezbollah fighters were reportedly brought to Iran, where Unit 8040 members participated in their reception and training. These activities demonstrate the unit's logistical and operational role in facilitating Iran's proxy warfare tactics.

The exposure of key figures such as Ghodratollah Fatemi and Rashid Bagheri, another individual linked to Unit 8040, indicates a concerted effort by external actors to undermine the unit's operations by targeting its leadership. Bagheri has been described as a "mercenary" involved in the 8000 unit, closely related to Unit 8040, showing that Unit 8040 operates within a broader organizational structure known as the 8000 Corps, which coordinates air defense and missile activities under the IRGC.

The unit's operations, particularly in training and deploying advanced missile systems such as the Sevom Khordad, underscore its critical role in enhancing Iran's air defense capabilities. The Sevom Khordad system, known for its ability to intercept advanced targets such as drones and fighter jets, has been deployed in various conflict zones, and Unit 8040's involvement in its development and deployment solidifies its strategic importance. The system gained international attention when it was reportedly used to down a U.S. Navy drone in 2019, further demonstrating its operational capabilities.

The detailed revelations about Unit 8040, its leadership, and its activities reflect the growing exposure of Iran's clandestine military units. Deliberately publicizing figures' identities like Fatemi and Bagheri suggests a targeted effort to disrupt Unit 8040's

operations and diminish its ability to function covertly. Despite this, the unit continues to play a pivotal role in Iran's defense strategy, contributing to both the protection of domestic missile infrastructure and the expansion of Iran's influence through proxy forces across the Middle East.

Unit 8040, under the command of Ghodratollah Fatemi, operates as a key player in Iran's air defense and missile strategy. Its responsibilities include the deployment and training of advanced systems such as the Sevom Khordad, support for proxy forces like Hezbollah, and involvement in regional conflicts in Syria and Lebanon. The unit's headquarters in Kashan and its additional operations in Garmdarreh and Tehran further highlight its expansive role in Iran's military infrastructure. Despite attempts to expose and disrupt its activities, Unit 8040 remains a cornerstone of Iran's defense and cyber warfare capabilities, solidifying its importance in regional and global military contexts.

Collaborations with Iranian Cyber Entities

Iran's cyber structure is decentralized, involving numerous contractors, academic institutions, and military units. Unit 8040 is likely working with -

Basij Cyber Battalions - Under the direct supervision of the IRGC, these battalions engage in cyber warfare that includes psychological operations, disinformation campaigns, and direct cyberattacks. Unit 8040 works closely with these battalions to coordinate cyber efforts, especially in air defense operations where cyber warfare is critical in securing or sabotaging airspace.

APT33, APT34, and APT35 - These well-known Iranian Advanced Persistent Threat groups have a track record of cyber espionage and sabotage campaigns targeting critical sectors such as energy, government, and defense. Unit 8040 could be integrated into these operations, particularly for missions targeting missile defense systems or military contractors developing anti-missile technologies.

Regional and Global Cyber Influence

Iran's strategy involves using cyberattacks and influence operations to project power regionally and globally. Unit 8040, while primarily focused on missile defense, is also likely contributing to broader IRGC efforts in these domains by -

Coordinating Cyberattacks in the Middle East - Unit 8040's cyber expertise is likely used to disrupt the military capabilities of regional rivals such as Saudi Arabia, the UAE, and Israel.

They have been known to execute cyber sabotage of military infrastructure, missile systems, and radar installations.

Cyber Espionage and Intelligence Gathering - The unit supports espionage efforts by leveraging its access to missile and air defense systems, helping gather critical intelligence from regional adversaries, including the interception of military communications and satellite data.

The Hezbollah Cyber Intelligence Unit

The Hezbollah Cyber Intelligence Unit highly likely collaborates closely with Unit 8040, given Hezbollah's reliance on Iran's cyber expertise and military support. As Iran's most prominent regional proxy, Hezbollah benefits directly from the cyber warfare capabilities and training provided by Iranian units like Unit 8040. With its specialization in missile defense, air defense systems, and cyber warfare, Unit 8040 likely plays a crucial role in enhancing Hezbollah's capabilities in UAV operations, cyber espionage, and electronic warfare.

In recent years, Hezbollah's cyber operations have advanced significantly, particularly in cyber surveillance, signals intelligence (SIGINT), and human intelligence (HUMINT). Unit 8040, which collaborates with Iranian APT groups like APT33 and APT34, is likely involved in supporting Hezbollah's cyber efforts through technical assistance and the transfer of advanced cyber tools. These APT groups are known for their role in proxy cyber operations, and Unit 8040's close relationship with them suggests a coordinated approach to boosting Hezbollah's cyber reach.

During conflicts like the Syrian Civil War, Unit 8040's involvement has extended to the ground, with reports indicating its personnel have been present in Lebanon and Syria. They provided Hezbollah with essential training and technical support, particularly in operating missile defense systems like the Sevom Khordad. This hands-on involvement highlights Unit 8040's central role in advancing Hezbollah's military and cyber capabilities, reinforcing their strategic partnership.

Unit 8040's role likely includes transferring sophisticated defense technology and systems to Hezbollah, ensuring that the group remains equipped with state-of-the-art physical and cyber warfare tools. The rise in Hezbollah's cyber proficiency, particularly in offensive and defensive operations, is attributed to Iran's advanced training and support, with Unit 8040 playing a pivotal role in these developments.

The Role of Contractors and Universities

Iran's cyber strategy often relies on external contractors and academic institutions to conduct its more sophisticated operations. Unit 8040, as a specialized unit, likely plays a role in guiding these efforts, particularly in areas requiring missile technology expertise. For example -

Imam Hossein University and Shahid Beheshti University have been linked to Iran's cyber operations, training hackers and developing cyber tools. Unit 8040 collaborates with these institutions to refine offensive tools, particularly those targeting air and missile defense systems.

While rooted in missile defense, unit 8040's offensive capabilities extend into cyber warfare by integrating with the IRGC's broader cyber operations. 8040's involvement in offensive cyber activities includes missile guidance sabotage, cyber espionage, targeted attacks on enemy defense systems, and collaboration with Iran's APT groups. These capabilities are a vital component of Iran's strategy to project power across the Middle East, ensuring that its military and proxy forces are protected from external threats while simultaneously degrading the capabilities of its enemies.

Comparative Analysis

A comparative analysis of Unit 8040's offensive cyber capabilities versus other components of Iran's cyber operations, let's break it down into key areas:

Aspect	**Unit 8040**	**Other IRGC Cyber Units (e.g., APT33, APT34, APT35)**	**Basij Cyber Battalions**
Primary Focus	Air defense and missile systems, with secondary involvement in offensive cyber operations	Focused on advanced persistent threats (APT), espionage, sabotage, and propaganda targeting critical sectors (energy, military contractors)	Psychological warfare, social media influence operations, and information warfare
Cyber Sabotage	Likely targets missile and air defense systems, particularly GPS spoofing and hacking enemy defense networks (e.g., Israel's Iron	APT33 and APT34 conduct destructive malware attacks (e.g., Shamoon, StoneDrill) aimed at critical	Engages in disinformation, trolling, and online influence campaigns against dissident groups, mainly targeting figures like Maryam Rajavi and groups such as MEK

Aspect	Unit 8040	Other IRGC Cyber Units (e.g., APT33, APT34, APT35)	Basij Cyber Battalions
	Dome, Saudi Arabia's Patriot)	infrastructure (energy sectors)	
Integration with APTs	Collaborates with APT groups (e.g., APT33, APT34, APT35) for cyber operations supporting military actions	Direct involvement in espionage and malware development, such as Shamoon used against Saudi targets	Coordination with IRGC in online disinformation campaigns, focusing on regime propaganda and psychological warfare
Targets	Enemy air defense systems and military infrastructure, supporting missile operations through cyber sabotage	Critical sectors, including oil and energy, government, and military contractors in Western countries	Dissident movements, opposition figures, and Western influence
Cyber Tools & Techniques	Uses tools for missile guidance disruption, hacking missile defense networks, and GPS spoofing	Development of custom malware (e.g., StoneDrill, Shamoon), spear-phishing, and ransomware	Social engineering, online trolling, and bot manipulation, especially on Twitter and other platforms
Collaboration with Universities & Contractors	Works closely with entities like Shahid Beheshti University and Imam Hossein University to refine cyber tools	Significant use of contractors like Mersad and ITSecTeam for sophisticated cyber operations	Coordination with student hackers and low-paid Basij members for cyber disinformation

Key Distinctions

- Unit 8040 focuses explicitly on missile systems and air defense cyber integration, which includes sabotage activities to disable enemy air defenses, distinct from APT groups that target broader critical sectors like energy.
- APT groups (e.g., APT33, APT34) focus more on developing advanced malware for espionage and long-term infiltration, whereas Basij units specialize in low-level disinformation campaigns and trolling.

- Unit 8040 is more likely to work with military-focused targets, while Basij Cyber Battalions deal with public opinion manipulation.

More on the Hezbollah Cyber Intelligence Unit

The Hezbollah Cyber Intelligence Unit plays a vital role within Hezbollah's broader military and espionage framework, benefiting significantly from Iranian support, especially from the IRGC and Iranian cyber units like Unit 8040. This unit conducts cyber operations, including surveillance, intelligence gathering, and cyberattacks aimed at Israel, Western countries, and regional adversaries. Its operations span various domains, from military cyber espionage to social media manipulation and information warfare.

The leadership of Hezbollah's Cyber Intelligence Unit aligns closely with Hezbollah's broader military and intelligence structure. Although specific names are often not publicly disclosed due to operational secrecy, it is clear that this unit operates under the strategic oversight of Hezbollah's senior leadership, including Hassan Nasrallah. Iran's influence over Hezbollah's cyber operations is facilitated through the IRGC and its Quds Force, which provides both strategic guidance and technological expertise. Leaders of Hezbollah's cyber operations maintain close coordination with their Iranian counterparts, reflecting the deep ties between the two entities.

Hezbollah's Cyber Intelligence Unit has developed considerable capabilities, primarily with Iranian assistance. Its cyber operations include:

- *Cyber Espionage: Hezbollah collects intelligence through advanced cyber surveillance, including signals intelligence (SIGINT) and human intelligence (HUMINT). Their operations involve intercepting communications, hacking into military and governmental systems, and gathering intelligence on adversaries like Israel and Saudi Arabia.*
- *Offensive Cyber Operations: Hezbollah has reportedly launched cyberattacks targeting Israel's infrastructure and military networks. These attacks often aim to disrupt communications, compromise sensitive information, and weaken military coordination.*
- *Propaganda and Influence Operations: The Cyber Intelligence Unit also spreads pro-Hezbollah narratives and anti-Western rhetoric, coordinating with Iranian-backed media outlets and using social media platforms to manipulate public opinion and gather support for Hezbollah's regional goals.*

Hezbollah's Cyber Intelligence Unit uses various social media platforms for propaganda and influence operations. Facebook, Twitter, Instagram, and Telegram are among the platforms where the group is most active, disseminating pro-Hezbollah and anti-Israel content, often in coordination with Iranian digital influence campaigns. Iran has been attributed with supporting Hezbollah's online propaganda, using both legitimate media outlets and fake accounts to amplify its messages. These operations often target audiences in Lebanon, Syria, and beyond, aiming to build support for Hezbollah's military actions and ideology.

Key figures within Hezbollah's leadership, influencing or overseeing its broader intelligence and cyber operations:

- *Hassan Nasrallah – As the Secretary-General of Hezbollah since 1992, Nasrallah plays a central role in overseeing all of Hezbollah's military, political, and intelligence operations. Given Hezbollah's tight control over its cyber activities, his leadership directly shapes the strategic goals of the Cyber Intelligence Unit.*
- *Talal Hamiyah – Hamiyah heads Hezbollah's External Security Organization and executes operations abroad, including cyber operations. His position suggests a significant role in overseeing the cyber campaigns that align with Hezbollah's international goals.*
- *Muhammad Kawtharani – A senior figure within Hezbollah's Political Council, Kawtharani is pivotal in coordinating Hezbollah's interests in Iraq and indirectly influencing cyber intelligence operations tied to those regional interests.*

The lethality of Hezbollah's Cyber Intelligence Unit lies in its ability to coordinate cyberattacks that degrade critical infrastructure and compromise military operations. By leveraging Iranian technology, Hezbollah has developed the capability to launch sophisticated cyberattacks that disrupt communications, command-and-control systems, and intelligence networks. Their cyber capability complements Hezbollah's broader military strategies, making it a formidable battlefield and cyberspace force. Its ability to conduct asymmetric warfare through cyber means adds a layer of complexity to its operational threat.

Hezbollah's Cyber Intelligence Unit, supported by Iran and aligned with Unit 8040's objectives, represents a growing cyber threat in the region. With advanced capabilities in cyber espionage, offensive cyber operations, and influence campaigns, the unit is a critical component of Hezbollah's strategy to weaken its adversaries, particularly Israel. Through

coordinated efforts with Iran, Hezbollah's cyber reach continues to expand, making it an essential element in the broader geopolitical landscape of the Middle East.

Infrastructure

Unit 8040's leadership, facilities, and operations are critical to Iran's broader cyber and military strategy, particularly within the IRGC's expansive network. Beyond Reza, who is often referenced as a significant figure in Unit 8040, other key players include prominent IRGC commanders, cyber coordinators, and strategic military locations involved in air defense and missile systems.

Hossein Hamedani, a former commander of the Tehran IRGC, played a pivotal role in the initial development of Iran's cyber warfare capabilities. As early as 2010, he reported that the Basij Cyber Council had trained over 1,500 cyber commandos, laying the foundation for the growing influence of cyber operations within the IRGC's military apparatus. Mohammad Pakpour, the current commander of the IRGC Ground Forces, oversees much of the IRGC's regional military engagements, including operations in Syria and Iraq. While not directly responsible for cyber operations, Pakpour's leadership highlights the interconnectedness of military and cyber strategies within the IRGC. These key figures demonstrate the hierarchical nature of Iran's cyber operations, with Unit 8040 positioned as a specialized unit within a much broader framework of Iranian military and intelligence efforts.

Several critical facilities are integral to Unit 8040's operations, notably Qeshm Island, Soga Air Base, and Lavizan-Shian. Qeshm Island houses a significant IRGC naval base, serving as a strategic point for missile batteries and a hub for Unmanned Aerial Vehicle (UAV) operations. The proximity to critical maritime routes in the Persian Gulf makes it crucial for military and cyber-related activities, particularly in monitoring and disrupting adversarial forces. Soga Air Base is another critical asset, functioning as a major center for coordinating missile systems and air defense operations. The airbase supports the IRGC's overarching objective of maintaining and enhancing Iran's missile capabilities, which Unit 8040 likely supports through cyber sabotage and resilience efforts. Lavizan-Shian, a facility that was once a military complex in Tehran and suspected of involvement in nuclear weapons research, continues to play a role in Iran's missile research and advanced weaponry, aligning with Unit 8040's expertise in missile systems and air defense.

The operational scope of Unit 8040 extends far beyond direct missile and air defense coordination. The Basij Cyber Battalions are crucial to Iran's cyber warfare strategy, engaging in low-level disinformation campaigns and psychological warfare. These battalions, spread across various provinces, are instrumental in the IRGC's broader efforts to control the narrative in both domestic and international spheres. By coordinating with Unit 8040 and

other IRGC cyber entities, the Basij engage in online campaigns that target opposition figures, particularly dissidents like Maryam Rajavi, while also attempting to disrupt the international perception of Iran. These efforts are primarily concentrated around Tehran, where Basij student units work alongside IRGC cyber coordinators to flood social media with regime-favorable content.

In addition to these cyber-focused operations, Unit 8040's activities are supported by a network of provincial commands across Iran. These 31 territorial IRGC commands manage cyber and military threats within their respective regions, often working closely with specialized brigades and cyber units to safeguard Iran's strategic interests. Locations like Tehran and Shiraz are key operational centers for the IRGC's Air and Space Force, which oversees Iran's missile capabilities and air defense. These centers will likely coordinate with Unit 8040 to secure missile systems against potential cyber intrusions while providing logistical and operational support for cyber sabotage efforts targeting adversarial missile defense systems.

October 7 Forward

Unit 8040 played a pivotal role in supporting Hamas during the events of October 7, 2023, and the subsequent conflict in Gaza. Unit 8040, operating under the IRGC's broader cyber and military framework, provided strategic assistance, enhancing the lethality and sophistication of Hamas's operations. Specifically, the unit provided missile technology, cyber sabotage tools, and advanced training that significantly upgraded Hamas's offensive and defensive capabilities.

Weapons and Technology Transfer

Unit 8040 has long been involved in transferring missile technology to Hamas, specifically enhancing their capacity to strike deeper into Israeli territory. On October 7, Hamas launched a coordinated missile barrage, the scale and precision of which can be linked to Iranian support, including from Unit 8040. The involvement of Iranian missile systems like the Fajr-5, previously supplied by Iran, played a critical role in saturating and overwhelming Israel's Iron Dome defense system.

Cyber Operations

Unit 8040's expertise in cyber warfare was also instrumental in disrupting Israeli military communications and infrastructure during and after the attack. Hamas's cyber unit, supported by Unit 8040, launched cyberattacks aimed at Israeli military and civilian networks, disrupting emergency response systems and causing widespread confusion. These operations were complemented by sabotage tactics

that targeted critical Israeli infrastructure, consistent with Iran's asymmetric warfare doctrine. Iranian-backed cyber efforts also extended to spreading disinformation across social media platforms, amplifying the psychological impact of the attacks.

Training and Coordination

Hamas militants received extensive training from Unit 8040, particularly in the use of UAVs (unmanned aerial vehicles) and missile deployment. This training included tactics for avoiding Israeli detection systems and maximizing the impact of strikes on both military and civilian targets. The Sevom Khordad missile defense system, a key asset within the Iranian military, was adapted for Hamas's use through training provided by Unit 8040. This collaboration allowed Hamas to deploy more advanced weapons with greater accuracy, further destabilizing Israeli defenses.

In summary, Unit 8040's involvement in the October 7 attack and subsequent operations in Gaza demonstrates its critical role in advancing Iran's regional proxy strategy. Through the provision of missile technology, cyber warfare expertise, and comprehensive training, Unit 8040 significantly amplified Hamas's operational capabilities, contributing to the unprecedented scale and sophistication of its attacks on Israel.

Thirty-One Territorial Commands

The 31 territorial commands of the IRGC cover Iran's provinces, each tasked with maintaining security, preparing for internal and external threats, and controlling local militia forces. The table below lists their names, locations, and primary functions:

Territorial Unit	Location	Primary Function
Tehran Command	Tehran	Central command is responsible for national operations, safeguarding political centers, and leading national defense efforts.
Mashhad Command	Mashhad, Razavi Khorasan	Handles security and military operations near the northeastern borders, focusing on threats from Afghanistan and Turkmenistan.
Kerman Command	Kerman	Manages southeastern Iran, focusing on internal unrest, smuggling, and cross-border insurgencies, especially near Pakistan.
Ahvaz Command	Ahvaz, Khuzestan	Defends the oil-rich southwest, manages operations near the Iraq border, and supports naval activities in the Persian Gulf.

Kermanshah Command	Kermanshah	Focuses on western Iran, particularly counterinsurgency operations and managing the volatile Kurdish region near Iraq.
Orumiyeh Command	Orumiyeh, West Azerbaijan	Defends the northwest, focusing on border security with Turkey and Azerbaijan and managing regional ethnic tensions.
Shiraz Command	Shiraz, Fars Province	Manages southern Iran, supporting missile and air defense systems and providing air support for naval defense in the Gulf.
Esfahan Command	Esfahan	A critical base for missile defense, managing Iran's central aerospace defense systems and ballistic missile deployments.
Dezful Command	Dezful, Khuzestan	Provides support for operations in southwestern Iran, including hosting UAV and missile operations for Gulf defense.
Tabriz Command	Tabriz, East Azerbaijan	Strategic command for operations along the Turkey-Azerbaijan border, focusing on regional security and air defense.
Birjand Command	Birjand, South Khorasan	Secures Iran's eastern borders with Afghanistan, focusing on air defense and monitoring border threats.
Qeshm Island Command	Qeshm Island, Persian Gulf	It supports missile and UAV operations and is critical for defending shipping lanes in the Strait of Hormuz.
Hormuz Island Command	Hormuz Island, Persian Gulf	Plays a crucial role in defending the Strait of Hormuz, including UAV and missile defense operations.
Bandar Abbas Command	Bandar Abbas, Hormozgan	Manages maritime defense, particularly UAV operations, and missile defense for the Strait of Hormuz.
Jask Command	Jask, Hormozgan	Strategic command for defending the Gulf of Oman and supporting naval and aerial surveillance.
Minab Command	Minab, Hormozgan	Provides UAV and missile support for southern coastal defense.
Mahshahr Command	Mahshahr, Khuzestan	Critical for naval defense operations in the Persian Gulf, managing UAV and missile defenses.
Bandar Imam Khomeini Command	Bandar Imam Khomeini, Khuzestan	Strategically crucial for Gulf defense, managing UAV and missile operations for regional security.
Chahbahar Command	Chahbahar, Sistan and Baluchestan	Provides naval support and UAV operations in the Arabian Sea, focusing on maritime security and surveillance.
Bandar Lengeh Command	Bandar Lengeh, Hormozgan	Manages coastal defense operations in the Persian Gulf, focusing on UAV and missile systems.
Ramsar Command	Ramsar, Mazandaran	Supports northern air defense operations, including UAV deployments.

Arak Command	Arak, Markazi Province	Critical for missile and UAV support in central Iran, particularly for defense within Iran's heartland.
Konarak Command	Konarak, Sistan and Baluchestan	Supports operations near the Gulf of Oman, particularly UAV and missile defenses.
Khorramabad Command	Khorramabad, Lorestan	Provides air defense and UAV support for operations in western Iran.
Shahroud Command	Shahroud, Semnan Province	Necessary to defend northeastern Iran's borders with UAV and air defense systems.
Lar Command	Lar, Fars Province	Manages UAV operations and air defense in southern Iran, critical for regional security.
Jiroft Command	Jiroft, Kerman Province	Key command for operations in southeastern Iran, supporting UAV and missile deployments.
Tabas Command	Tabas, South Khorasan Province	Supports air defense and UAV operations near Iran's eastern borders, critical for security along the Afghan frontier.
Seman Command	Semnan Province	Manages missile testing and UAV development, vital for Iran's aerospace operations.

Direct Ties to Hamas

Unit 8040's collaboration with Hamas operates within the framework of Iran's strategic goals, mainly through the IRGC's extensive network. Unit 8040, with its focus on cyber warfare and missile defense, has directly contributed to enhancing the capabilities of Hamas, mainly through its military wing, the Izz ad-Din al-Qassam Brigades. This collaboration has resulted in technological and tactical advancements for Hamas, notably in cyber warfare, missile technology, and UAV operations.

Hamas' cyber wing has grown substantially with Iranian support. The expertise provided by Unit 8040 has enabled Hamas' Cyber Intelligence Unit to launch significant cyber operations, such as coordinated hacking campaigns and surveillance efforts, targeting Israel and regional adversaries, mirroring the longstanding ties between the IRGC and Hamas, with Unit 8040 as a conduit for training and technical support.

On the military front, Unit 8040 has been instrumental in providing Hamas with missile expertise, including the technology behind Iranian missile systems like the Fajr-5. This support has allowed Hamas to increase the range and precision of its rocket arsenal, enabling it to strike deeper into Israeli territory. Unit 8040's assistance has also played a role in the Sevom Khordad missile defense system training, which is passed on to Hamas militants, ensuring that Hamas maintains its deterrence posture against Israeli air strikes.

Moreover, Unit 8040 has been tied to the transfer of cyber expertise to Hamas, allowing them to engage in sophisticated cyber espionage, DDoS attacks, and the disruption of Israeli infrastructure. With Iran's backing, Hamas' cyber operations have become more aggressive and far-reaching, targeting both civilian and military assets. This operational synergy between Unit 8040 and Hamas highlights the IRGC's broader strategy of using cyber warfare as an extension of its asymmetric warfare tactics.

In conclusion, Unit 8040's support has dramatically strengthened Hamas' military and cyber capabilities, making it a more formidable adversary for Israel and contributing to the broader regional objectives of Iran's proxy network.

A Specialized Component

Unit 8040 is a specialized component within Iran's broader cyber and missile defense strategy, closely tied to the IRGC's overarching command structure. While traditionally focused on air defense and missile operations, Unit 8040 has demonstrated significant offensive cyber capabilities, particularly in securing Iran's missile systems and conducting cyber-sabotage aimed at enemy defense infrastructure. Unit 8040 is likely integrated into the IRGC's growing cyber operations, with responsibilities that include disrupting missile defense systems like Israel's Iron Dome or Saudi Arabia's Patriot systems.

The leadership of Unit 8040 fits within the larger IRGC hierarchy, where senior commanders with deep experience in Iran's military structure oversee operations. While Reza is often referenced as a leader within this unit, other key figures within the IRGC, such as Mohammad Pakpour and Hossein Hamedani, have contributed to the unit's expansion and integration with other military branches. These leaders draw upon their experience from past conflicts, such as the Iran-Iraq War, and bring a focus on asymmetric warfare that defines much of Unit 8040's strategic operations.

Geographically, Unit 8040 operates from several facilities, with strategic locations like Qeshm Island and the Parchin Military Complex playing pivotal roles in its missile defense operations. Qeshm Island, situated near the Strait of Hormuz, is a critical hub for missile defense and UAV operations, while Parchin supports more clandestine research and development activities related to missile technology. Other facilities, such as Soga Air Base and sites in Tehran, contribute to the operational efficiency of Unit 8040, integrating air defense with Iran's cyber capabilities.

Unit 8040's integration with APT groups, such as APT33 and APT34, expands its operational scope beyond traditional military activities. These groups provide the necessary cyber expertise to conduct reconnaissance, long-term espionage, and sabotage operations. Unit

8040 coordinates with these cyber groups, particularly in missions that target enemy missile systems and critical infrastructure. Iranian cyber tools like Shamoon and StoneDrill have been employed in past operations, demonstrating Unit 8040's access to sophisticated malware designed to wipe data or disable enemy systems.

The structure of Iran's military decentralization enhances Unit 8040's capabilities. The 31 territorial commands of the IRGC are spread across Iran, each tasked with regional defense and supporting broader military goals. These commands work with Unit 8040 to ensure regional stability while bolstering Iran's missile defense network. Locations such as Mashhad, Kerman, and Ahvaz are key operational centers that link local defense needs with national security interests. These territorial commands provide the staffing and logistical support necessary for Unit 8040 to conduct offensive and defensive cyber operations.

Unit 8040's responsibilities align closely with Iran's broader military doctrine, emphasizing asymmetric warfare and mosaic defense. Its cyber operations serve to disrupt and disable enemy air defense systems, weakening adversarial capabilities in the event of a military confrontation. In addition to preemptive strikes, Unit 8040 plays a role in defending Iran's missile infrastructure from potential cyber intrusions. This dual focus on offense and defense ensures that Unit 8040 remains a critical component of Iran's cyber and military strategy.

Wrap Up

Unit 8040 is a critical force within Iran's cyber and missile defense strategy, showcasing the country's ability to blend traditional military operations with advanced cyber capabilities. Under the leadership of Ghodratollah Fatemi, the unit has evolved beyond its initial focus on air defense, expanding into offensive cyber operations that target enemy defense systems like Israel's Iron Dome and Saudi Arabia's Patriot batteries. Through its collaboration with Iranian APT groups such as APT33 and APT34, Unit 8040 has enhanced its role in cyber espionage, sabotage, and reconnaissance, allowing it to disrupt adversarial military operations and protect Iran's strategic assets. Its close ties with Hezbollah, particularly in training and equipping the group's cyber intelligence unit, further amplify Iran's regional influence.

The integration of Unit 8040 into the broader IRGC structure, along with its operations from vital strategic locations like Qeshm Island and the Shahid Karimi base in Kashan, underscores its importance in national defense and proxy warfare. By providing critical support to Hezbollah and other Iranian-aligned groups, Unit 8040 ensures that Iran's cyber and missile capabilities extend far beyond its borders. The unit's activities exemplify Iran's

asymmetric warfare doctrine, combining cyber operations with traditional military tactics to project power and maintain regional dominance. As Iran continues to expand its cyber warfare capabilities, Unit 8040 will remain a pivotal player in shaping the future of the country's military and geopolitical strategies.