Mahdi Lashgarian

Position: Senior Official, Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC)
Affiliation: Islamic Revolutionary Guard Corps (IRGC), CyberAv3ngers

---

Mahdi Lashgarian operates as a senior officer within the Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC), a specialized unit responsible for offensive cyber operations and electronic warfare aligned with Iran's national security agenda. Alongside five other prominent IRGC cyber officials, Lashgarian forms a core leadership structure, directing various cyber campaigns primarily aimed at disrupting critical infrastructure in nations perceived as hostile, notably the United States and its allies.

Key Responsibilities and Operations

Lashgarian oversees numerous cyber operations through CyberAv3ngers, a hacking group reportedly functioning as a front for IRGC cyber activities. This group has targeted programmable logic controllers (PLCs) manufactured by the Israeli company Unitronics, which are used extensively across U.S. sectors such as water treatment, wastewater management, and energy. In 2023, under Lashgarian's strategic leadership, CyberAv3ngers compromised PLCs linked to multiple U.S. water utilities, including a significant breach at the Municipal Water Authority of Aliquippa, Pennsylvania. These incidents forced utility operators to shift to manual operations to mitigate potential risks to water quality and public safety

Cyber Techniques and Tactics

Lashgarian's expertise lies in orchestrating complex intrusion techniques that exploit vulnerabilities in industrial control systems (ICS). CyberAv3ngers, under his guidance, has employed sophisticated malware and social engineering tactics to access PLCs and other ICS equipment, often capitalizing on default or weak security configurations. By compromising the PLCs, CyberAv3ngers gains control over essential infrastructure processes, enabling potential shutdowns, data exfiltration, or deliberate system malfunctions, though their operations are frequently designed to evade immediate detection

Recent Sanctions and International Response

In February 2024, the U.S. Treasury Department sanctioned Mahdi Lashgarian, along with five other IRGC-CEC leaders, labeling their cyber campaigns “unconscionable” and “dangerous.” These sanctions freeze all assets linked to Lashgarian in the United States and prohibit U.S. individuals and entities from engaging in transactions with him. Additionally, the U.S. State Department’s Rewards for Justice program offers a reward of up to $10 million for information leading to his identification or location, underscoring the global importance placed on countering his cyber activities.

Strategic Focus and Influence Operations

Lashgarian contributes extensively to influence and information operations aimed at destabilizing political climates in targeted countries. His role involves coordinating cyber intrusions with broader IRGC influence campaigns, leveraging digital media platforms to disseminate misinformation that amplifies social divisions or supports Iranian geopolitical narratives. His influence operations have targeted critical moments, such as U.S. electoral periods and regional protests, to further Iran’s strategic interests through psychological manipulation and propaganda.

Background and Skills

Lashgarian possesses significant technical knowledge in ICS and SCADA (Supervisory Control and Data Acquisition) systems, particularly regarding their vulnerabilities and integration in critical infrastructure. His understanding of malware development and exploitation tactics has enabled CyberAv3ngers to adapt tools used by known Iranian APT groups, including APT33 and APT34, optimizing them for espionage and sabotage missions. Lashgarian’s dual focus on cyber disruption and psychological influence exemplifies the IRGC-CEC’s hybrid warfare approach, which blends cyber operations with psychological tactics.

Mahdi Lashgarian represents a leading figure in Iran’s state-sponsored cyber warfare initiatives. His role in directing operations against critical infrastructure and coordinating influence campaigns reveals a strategic intent to exert influence far beyond Iran’s borders. Through CyberAv3ngers, Lashgarian has become a significant threat to cybersecurity frameworks in countries targeted by IRGC cyber operations. International sanctions and heightened intelligence measures now focus on countering his activities, aiming to neutralize one of Iran's most persistent cyber threats.

Mohammad Bagher Shirinkar
Alias: Mojtaba Tehrani
Affiliation: Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC), Emennet Pasargad, Sayyad Project

---

Overview

Mohammad Bagher Shirinkar, also known by the alias Mojtaba Tehrani, is an influential operative within the Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC). Shirinkar manages significant Iranian cyber warfare operations, notably through his role at Emennet Pasargad, a state-linked company central to IRGC's cyber strategies. His sanctioned status reflects an active involvement in numerous global cyber intrusions and influence campaigns, particularly targeting adversaries' infrastructure, foreign governments, and public perception abroad.

Professional Background and Strategic Responsibilities

Shirinkar has led numerous operations aimed at strategic infrastructure disruption and information warfare, functioning within a tightly controlled IRGC apparatus. He has managed or overseen attacks aimed at U.S., Israeli, and European assets, often leveraging his company Emennet Pasargad. As a leader within the IRGC-CEC, Shirinkar orchestrates cyber missions aligned with broader Iranian security objectives, focusing on creating systemic disruptions and discrediting Iran's international opponents.

At Emennet, Shirinkar has supervised initiatives such as data exfiltration and critical infrastructure breaches, with a noted focus on programmable logic controllers (PLCs) in water treatment and other critical sectors. His activities involve collaboration with skilled teams within the IRGC to employ malware, including ransomware, and other tactics to infiltrate and disrupt targeted systems abroad.

High-Profile Operations

Shirinkar's operational influence is evident in several cyber-attacks attributed to the IRGC's cyber apparatus, including the Sayyad Project, which targeted the Albanian government's infrastructure in response to the hosting of Iranian dissident groups. In this operation, hackers employed malware to exfiltrate sensitive government information, disrupt public services, and release stolen data through affiliated online channels. Shirinkar reportedly coordinated closely with IRGC intelligence networks to ensure alignment with strategic Iranian interests

منیبان

اسپوتنیک ایران

U.S. Department of the Treasury

ایران اینترنشنال

.

IRGC and Sanctions

International sanctions reflect Shirinkar's role in cyber operations that disrupt foreign critical infrastructure. The U.S. Treasury and international organizations have cited Shirinkar’s activities within Emennet and his alleged support of IRGC intelligence projects, identifying him as a key contributor to destabilizing cyber campaigns. Sanctions specifically target Shirinkar’s facilitation of attacks that aim to create both physical and psychological impacts on targeted nations. His link to IRGC’s overarching cyber intelligence tactics demonstrates his deep integration within Iran’s state-sponsored cyber agenda.

Network and Collaboration

Shirinkar operates within a tight circle of IRGC officials, including his brother Mohammad-Hossein Shirinkar, who holds a parallel role within the IRGC Intelligence Inspectorate. Together, they engage in joint ventures that exploit weaknesses in international infrastructure, relying on a coordinated network of cyber assets and intelligence. Additional family members, including Mehdi Hashemi Tughraljardi, further extend Shirinkar's influence within Iran’s cyber operations, adding layers of operational support to IRGC cyber initiatives

ایران اینترنشنال

.

Skills and Techniques

Shirinkar’s proficiency spans ICS exploitation, malware customization, and social engineering. Under his direction, teams conduct spear-phishing campaigns targeting critical infrastructure personnel. He applies these skills strategically to access systems controlling essential resources like water and energy. His involvement in malware

development and influence tactics illustrates his commitment to integrating cyber and psychological warfare elements to achieve IRGC's objectives.

Mohammad Bagher Shirinkar represents a critical figure in Iran's cyber warfare landscape, blending technical skills with a commitment to advancing IRGC's cyber and geopolitical objectives. His actions have placed him among Iran's most targeted cyber operatives, with sustained sanctions and intelligence monitoring from international authorities.

Reza Mohammad Amin Saberian
Senior Cyber Operations Official, IRGC Cyber-Electronic Command (IRGC-CEC)

Personal Information

- **Date of Birth**: February 1, 1980
- **Nationality**: Iranian
- **Passport**: G10515157 (expires October 5, 2024)
- **National ID Number**: 2431884694

Professional Overview
Reza Mohammad Amin Saberian is a prominent figure in the Iranian cyber landscape, functioning as a senior official within the Cyber-Electronic Command (CEC) of the Islamic Revolutionary Guard Corps (IRGC). Known for his deep involvement in strategic cyber activities, Saberian has played a pivotal role in several high-profile cyber operations orchestrated by Iran's cyber apparatus. His work aligns with the IRGC's objectives to advance Iran's geopolitical influence through offensive cyber tactics, often aimed at undermining critical infrastructure in countries perceived as adversaries.

Role and Responsibilities
In his capacity as a senior official, Saberian is instrumental in coordinating and supervising cyber activities against critical infrastructure targets. His efforts focus on advancing Iran's cyber capabilities, particularly in developing sophisticated tools tailored for industrial control systems (ICS) and supervisory control and data acquisition (SCADA) environments. These systems are integral to the operations of essential facilities such as water, energy, and transportation sectors in various countries, including the United States, Israel, and European nations.

Saberian's expertise covers malware development, advanced intrusion techniques, and the orchestration of cyber-physical integration, enabling comprehensive and multi-layered attack strategies. His operations often involve close collaboration with other high-ranking

officials within the IRGC-CEC, including those managing affiliated hacking groups, such as CyberAv3ngers. This group has gained notoriety for deploying ransomware, defacement, and data manipulation attacks targeting water facilities and programmable logic controllers (PLCs).

Notable Cyber Operations

1. **Unitronics PLC Attacks** (2023-2024):
   Saberian directed cyberattacks on Unitronics PLC systems, manufactured by an Israeli company, during a period of heightened geopolitical tension. These attacks targeted water utilities in the United States and several critical infrastructure sites. By exploiting vulnerabilities in ICS technologies, Saberian's team attempted to control processes within water treatment facilities, highlighting the IRGC's ability to breach core infrastructure. While the attacks caused temporary disruption, emergency response teams were able to mitigate broader impacts.

2. **Ransomware Deployment and Defacement Campaigns**:
   Saberian's operations frequently employ ransomware attacks, notably targeting municipal and healthcare facilities. One high-profile incident involved hacking systems at a Pennsylvania water utility, where attackers took systems offline and forced manual operations. Messages left on the defaced systems underscored the political motivations behind the attacks, aligning with Iran's broader anti-Western cyber narrative.

3. **Influence Operations and Data Manipulation**:
   Working alongside other IRGC entities, Saberian has managed initiatives focused on spreading misinformation and influencing public perception in targeted regions. His influence tactics include amplifying anti-U.S. sentiments through social media channels and conducting phishing attacks to compromise high-profile accounts in sensitive sectors.

Technical Capabilities and Expertise

Saberian's skills encompass malware engineering for ICS and SCADA systems, secure command and control (C2) communications, and advanced encryption protocols that enhance the stealth and resilience of IRGC cyber tools. His technical acumen allows him to oversee the design and implementation of persistent threats capable of infiltrating and manipulating core operations within infrastructure networks. This expertise reflects Iran's commitment to developing a self-sufficient cyber warfare capability resistant to foreign countermeasures.

Sanctions and International Response
In February 2024, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) designated Saberian, along with five other senior IRGC-CEC officials, under sanctions for malicious cyber activities against critical infrastructure. These sanctions restrict his access to financial networks and assets within U.S. jurisdictions and signal intensified international scrutiny of Iran's cyber campaigns. The U.S. Rewards for Justice program also offers up to $10 million for information on Saberian's activities, underscoring the international concern regarding his role in destabilizing cyber operations.

Public Image and Media Depictions
Within Iran, state-affiliated sources and media present Saberian and his colleagues as protectors of national security, countering foreign threats through defensive cyber measures. Outlets like *Khabar Online* and *Sputnik Iran* frequently describe IRGC cyber activities as protective, often downplaying accusations from Western authorities. Iranian news agencies frame Saberian's actions as countermeasures to protect Iran's sovereignty and integrity against perceived foreign aggressions, reinforcing his standing as a dedicated figure within Iran's defense sector.

Educational and Training Background
While specific details on Saberian's formal education remain undisclosed, his background likely includes advanced technical training in computer science, cybersecurity, and network engineering at Iran's elite military institutions. Given his rank and responsibilities, Saberian's training possibly included specialized programs at institutions linked to the IRGC, focusing on secure software development, ICS vulnerabilities, and tactical cyber operation management. This education has prepared him to handle complex, large-scale cyber missions that target both regional and global adversaries.

Reza Mohammad Amin Saberian exemplifies the technical prowess and operational depth characterizing Iran's cyber warfare strategies. His career within the IRGC-CEC marks him as a figure central to Iran's offensive cyber posture, with a record of operations that underscore the IRGC's capabilities and ambitions on the global stage. Through sophisticated cyberattacks and calculated targeting, Saberian plays a significant part in shaping Iran's influence in cyberspace, challenging adversarial infrastructure, and advancing IRGC's strategic objectives.

Hamid Homayunfal
Position: Senior Cybersecurity Officer, Islamic Revolutionary Guard Corps Cyber-

Electronic Command (IRGC-CEC)
Nationality: Iranian

Overview

Hamid Homayunfal operates as a prominent figure within the IRGC's Cyber-Electronic Command (IRGC-CEC). His role involves spearheading sophisticated cyber initiatives, focusing on cyber-intrusion tactics aimed at both national and international targets. Homayunfal's name gained attention following sanctions imposed by the U.S. Treasury Department in 2024, citing his involvement in cyber campaigns against critical infrastructure across multiple countries. The U.S. identifies him as a leading architect in campaigns that target the energy, water, and transportation sectors globally.

Role and Responsibilities

Homayunfal leads IRGC cyber operations that focus on advanced malware deployment, network intrusion, and data manipulation. His work involves strategic oversight of operations aimed at identifying vulnerabilities within foreign industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. His leadership extends to supervising attacks on infrastructures such as water treatment facilities and energy grids in perceived adversarial countries.

Reports indicate that Homayunfal collaborates with specialized units within the IRGC-CEC, including groups like CyberAv3ngers. His team conducts spear-phishing campaigns targeting key personnel in critical sectors, often using custom-designed malware capable of persistent access. As part of his role, he works with IRGC's malware developers to craft tools that exploit weak points in essential infrastructure systems, allowing for extensive network infiltration and surveillance.

Key Operations

1. **ICS and SCADA Attacks**
   Under Homayunfal's direction, the IRGC launched a series of cyber-attacks targeting SCADA systems in sectors such as water treatment and electrical grids. By exploiting technical vulnerabilities in U.S. and Israeli infrastructures, Homayunfal's team sought to disrupt and monitor critical systems, indicating a capacity for long-term cyber disruption.

2. **Critical Infrastructure Campaigns in the United States**
   Hamid Homayunfal reportedly oversaw attacks targeting U.S. water treatment facilities, with evidence suggesting efforts to alter chemical levels in water supplies. This campaign included both reconnaissance and offensive actions, enabling IRGC

hackers to understand system architecture before attempting more severe disruptions. His teams frequently used ransomware as a secondary tactic, often embedding messages with anti-Western propaganda.

3. **Influence Operations Coordination**
   Homayunfal also played a role in Iran's influence operations, using social media and fake accounts to amplify anti-U.S. and anti-Israel narratives. His expertise in crafting cyber-influence tactics complements his technical skills in cyber-warfare, making him an effective operative within the IRGC's hybrid warfare model.

Technical Expertise and Capabilities

Homayunfal's technical skill set covers ICS malware engineering, network penetration, and secure communications protocols. He demonstrates particular expertise in designing malware that adapts to various ICS and SCADA environments, ensuring persistent network access and the ability to remotely control operations. His team uses encrypted command-and-control channels that enhance the resilience of their operations against foreign cybersecurity defenses.

His knowledge of social engineering tactics also enhances the IRGC's cyber capabilities, as he frequently directs campaigns that blend technical infiltration with deception techniques to compromise targeted infrastructures.

Sanctions and International Impact

The U.S. Treasury's Office of Foreign Assets Control (OFAC) sanctioned Homayunfal in 2024, placing him among a group of five Iranian officials connected to IRGC cyber initiatives. Sanctions cite his role in "malicious cyber operations against critical infrastructures" across the U.S., Israel, and Europe. OFAC's designation also freezes any U.S.-linked assets and restricts his access to financial resources in an attempt to curb his operations.

Internationally, Hamid Homayunfal is monitored by intelligence agencies concerned with Iran's cyber influence. His activities reinforce Iran's strategic cyber ambitions, which aim to leverage infrastructure attacks as a means to exert pressure on perceived adversaries.

Background and Training

Homayunfal likely received training in Iran's elite military academies, specializing in cybersecurity, electronic warfare, and industrial control systems. His education likely emphasizes both technical skills and operational secrecy, equipping him with the knowledge necessary for high-stakes cyber missions. With a focus on subverting foreign

infrastructure, Homayunfal's training allows him to oversee the implementation of large-scale cyber operations that align with IRGC strategic goals.

Hamid Homayunfal remains a significant figure within Iran's state-sponsored cyber warfare initiatives. His coordination of high-impact cyberattacks, combined with his technical expertise in malware and ICS/SCADA infiltration, underscores his value within the IRGC's offensive cyber framework. Through his work, he contributes to IRGC-CEC's ability to disrupt and surveil adversarial infrastructure, cementing his position within Iran's cybersecurity and cyber warfare operations.

Hamid Reza Lashgarian
Position: Commander, IRGC Cyber-Electronic Command (IRGC-CEC)
Nationality: Iranian
Date of Birth: March 21, 1961

Overview

Hamid Reza Lashgarian leads the Cyber-Electronic Command of Iran's Islamic Revolutionary Guard Corps (IRGC). His role centers on overseeing complex cyber operations targeting foreign critical infrastructure, including industrial control systems (ICS) within essential sectors such as water, energy, and transportation. Lashgarian's work is instrumental in advancing Iran's offensive cyber capabilities, aligning closely with Iran's broader strategic goals under the IRGC's mandate.

Professional Background and Key Responsibilities

As head of the IRGC-CEC, Lashgarian directs cyber campaigns that support IRGC's strategic initiatives, targeting perceived adversaries. He has structured the IRGC-CEC to deploy advanced tactics, including custom-designed malware tailored to penetrate ICS and SCADA systems integral to national infrastructure operations. His role involves not only the development and deployment of technical attack tools but also close coordination with entities such as Iran's Quds Force, which focuses on military and espionage operations abroad.

Reports indicate that Lashgarian plays a central role in high-level cyber-physical integration, where he aligns cyber tactics with Iran's military objectives. His leadership has led to notable cyber incidents that highlight Iran's capabilities in targeting foreign infrastructures. Recent U.S. sanctions have cited Lashgarian and his operations as direct threats to global stability due to the high-impact nature of the attacks.

Major Cyber Operations and Strategic Impact

1. **CyberAv3ngers and ICS Targeting**
   Lashgarian coordinates closely with CyberAv3ngers, an IRGC-aligned hacking group responsible for attacking critical infrastructure components, including U.S. water facilities. His directive enabled CyberAv3ngers to exploit vulnerabilities in PLCs, particularly those manufactured by Israeli companies such as Unitronics, which serve as core control elements in water treatment systems. Through these actions, his unit has demonstrated an ability to infiltrate and manipulate key infrastructure assets.

2. **Influence Operations During U.S. Elections**
   Under Lashgarian's guidance, the IRGC-CEC orchestrated online influence campaigns that exploited social media and other digital channels to spread disinformation aimed at destabilizing political climates abroad. His teams have conducted coordinated misinformation campaigns intended to amplify divisions within U.S. society and counteract narratives unfavorable to Iran, especially during sensitive periods like the U.S. election cycle.

3. **International Coordination with IRGC's Quds Force**
   Lashgarian has facilitated collaboration between IRGC-CEC and the Quds Force, enabling cyber operations to complement military missions. This includes strategic use of cyber tactics to undermine adversaries' defenses and engage in intelligence-gathering activities supporting broader IRGC objectives. His expertise in hybrid warfare is evident in operations that combine cyber sabotage with physical threats, targeting both regional and international entities.

Technical Expertise and Strategic Capabilities

Lashgarian's expertise spans malware development, secure command-and-control (C2) protocols, and exploitation of ICS-specific vulnerabilities. His leadership in engineering custom malware aligns with a focus on persistence and resilience in hostile network environments. Lashgarian's deep understanding of cyber tactics enables him to execute operations that evade detection while delivering maximum operational impact on targeted infrastructures.

Lashgarian's unit has developed cyber tools capable of embedding within essential control systems, thus allowing remote operational disruption and data exfiltration. His team's access to high-level encryption and secure C2 frameworks enables them to conduct prolonged intrusions with reduced risk of exposure.

Academic Background and Public Perception

As a former assistant professor at Imam Hossein University, Lashgarian has published extensively on cybersecurity and electronic warfare, contributing to IRGC's doctrine on cyber warfare. His academic background reflects a strong foundation in both theoretical and practical aspects of cyber tactics, particularly in military contexts. Iranian media, including outlets like *Sputnik Iran* and *Khabar Online*, portray Lashgarian's work as defensive, emphasizing his role in countering perceived foreign aggression.

Sanctions and International Response

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned Lashgarian in February 2024, labeling him as a high-level operative in Iran's offensive cyber campaigns. Sanctions specifically target his activities related to critical infrastructure attacks, which have reportedly led to destabilizing impacts on U.S. and allied systems. OFAC's designation restricts Lashgarian's access to financial resources and blocks assets within U.S. jurisdictions. Additionally, the Rewards for Justice program offers $10 million for information leading to Lashgarian, underscoring international concern over his activities.

Personal Information

Reports from Iranian and international sources, including *Iran International*, indicate that Lashgarian resides in Tehran. His family connections have occasionally surfaced, with his wife reportedly working at Evin Prison, as noted in sources describing interactions between Iranian officials and detainees.

Hamid Reza Lashgarian exemplifies the IRGC's cyber warfare capabilities, with a career dedicated to advancing Iran's offensive cyber strategies. His leadership within the IRGC-CEC reflects a systematic approach to hybrid operations, merging cyber tactics with military objectives to secure Iran's strategic interests. Through a blend of technical skill, operational oversight, and cross-functional collaboration, Lashgarian reinforces the IRGC's position as a formidable cyber power targeting adversarial infrastructure globally.

Milad Mansuri
Position: Senior Official, IRGC Cyber-Electronic Command (IRGC-CEC)
Nationality: Iranian
Date of Birth: September 11, 1989

Profile Overview

Milad Mansuri holds a prominent position within the Islamic Revolutionary Guard Corps' Cyber-Electronic Command (IRGC-CEC), where he contributes extensively to Iran's cyber strategy, focusing on targeting critical infrastructure abroad. His work involves the design

and deployment of complex cyber attacks, particularly those that exploit vulnerabilities in industrial control systems (ICS) across sectors that are pivotal to national security.

Professional Background and Responsibilities

In his capacity as a senior IRGC-CEC figure, Mansuri has been instrumental in directing operations that align with Iran's strategic cyber and intelligence objectives. His role entails overseeing the development of malware and other cyber tools used to infiltrate essential systems, including Programmable Logic Controllers (PLCs) in the water and energy sectors. Mansuri's focus on high-value targets has made him a crucial asset in the IRGC's efforts to apply pressure on adversarial states by compromising sensitive infrastructure.

Reports indicate that Mansuri coordinates extensively with IRGC-affiliated hacking teams, particularly CyberAv3ngers, which has executed a series of cyber campaigns aimed at disrupting foreign infrastructure. His approach emphasizes exploiting weaknesses in Israeli-made PLC systems, which are widely used in U.S. facilities. Such operations not only target operational technology but also aim to send a political message aligned with Iran's broader geopolitical stance.

Major Cyber Operations and Strategic Impact

1. **Operation Against U.S. Water Facilities**
   Mansuri's team orchestrated a significant attack on U.S. water infrastructure in 2023, including a cyber incident at the Aliquippa Water Authority in Pennsylvania. CyberAv3ngers, operating under Mansuri's guidance, compromised Israeli-manufactured Unitronics PLCs, projecting anti-Israel messages and demonstrating their access capabilities. Although the specific event did not result in major disruption, it highlighted vulnerabilities within critical infrastructure and underscored Iran's ability to penetrate and manipulate operational systems remotely.

2. **Ransomware Campaigns Targeting Healthcare and Financial Sectors**
   Mansuri has also been linked to ransomware campaigns targeting Western healthcare and financial institutions, where cyber disruptions have a high potential for operational and economic impact. His strategies have reportedly involved ransomware attacks that encrypt sensitive data and demand high-value payouts, effectively creating financial and logistical pressures on targeted institutions. These campaigns underscore a shift in IRGC tactics towards economically motivated cyber extortion.

3. **Social Engineering and Initial Access Operations**
   In addition to technical malware development, Mansuri's work includes directing

social engineering campaigns that facilitate initial network access. His team has designed spear-phishing campaigns with customized lures to deceive employees within targeted sectors, establishing footholds that allow IRGC-CEC operatives to initiate more extensive infiltrations. These phishing tactics reflect a deep understanding of Western corporate and governmental network structures.

Technical Expertise and Strategic Capabilities

Mansuri possesses specialized expertise in ICS vulnerabilities, particularly in the engineering and adaptation of malware that can sustain prolonged infiltration and control within these systems. His proficiency extends to the development of secure command-and-control (C2) channels, which maintain covert communication with compromised devices while evading detection by conventional security protocols.

Educational Background and Public Perception

While details about Mansuri's educational background remain limited, his expertise indicates advanced training in cybersecurity and network exploitation. Iranian state-aligned media portray Mansuri's cyber activities as part of Iran's defensive posture, framing his work as a necessary countermeasure against foreign threats. Outlets such as *Khabar Online* and *Sputnik Iran* frequently characterize Mansuri's cyber campaigns as actions against Western technological dominance, emphasizing their defensive narrative.

Sanctions and International Response

In February 2024, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned Mansuri along with other IRGC-CEC officials for his involvement in recent cyber attacks targeting critical infrastructure. Sanctions restrict Mansuri's access to assets in U.S. jurisdictions and block financial transactions associated with him, underscoring the perceived threat his operations pose to global security. Furthermore, the Rewards for Justice program offers a substantial bounty for information leading to Mansuri, highlighting his significance within IRGC's cyber hierarchy.

Personal Information and Notable Associations

Milad Mansuri remains largely private regarding personal details; however, his association with other senior IRGC-CEC officials, such as Hamid Reza Lashgarian and Mohammad Bagher Shirinkar, places him at the center of Iran's coordinated cyber strategy. Reports suggest Mansuri has operational connections to technical experts within IRGC-affiliated companies that assist in malware development, creating a cohesive network supporting IRGC-CEC's offensive capabilities.

Milad Mansuri exemplifies the IRGC's approach to cyber warfare, blending technical expertise with strategic objectives that seek to compromise adversaries' critical infrastructure. His work within the IRGC-CEC reflects a methodical approach to both cyber infiltration and ransomware operations, positioning him as a central figure in Iran's pursuit of cyber dominance and control. Through continuous adaptation of tactics and advanced malware engineering, Mansuri reinforces Iran's capacity to challenge and disrupt global systems while advancing the IRGC's geopolitical goals.

Details from Iranian Media Outlets

Khabar Online

Khabar Online, a well-read Iranian media outlet, frequently highlights the defensive nature of Iran's cyber strategies. Commentaries in this publication describe Mansuri's involvement in cyber initiatives as fundamentally protective, emphasizing that Western countries, particularly the U.S., exaggerate Iranian cyber activities. Articles suggest that individuals like Mansuri are unfairly targeted by sanctions and foreign media, which, according to Khabar Online, misrepresent Iran's motives to justify geopolitical pressures against the country

Khabar Online

One article from 2023 specifically comments on the U.S. sanctions imposed on IRGC cyber officials, describing these measures as a reflection of Western double standards. It argues that while the West itself engages in extensive cyber operations, it publicly denounces any defensive responses from countries like Iran. This piece underscores that officials like Mansuri and his associates are fulfilling state-assigned roles to shield Iran from foreign digital interference and bolster domestic cybersecurity infrastructure, defending national sovereignty rather than pursuing offensively-driven actions.

Sputnik Iran

Sputnik Iran, affiliated with the Russian state media agency, shares a similar perspective, often aligning with narratives that counter Western depictions of Iranian cyber activities. Sputnik Iran frequently publishes opinions and analyses that characterize Iran's cyber initiatives as part of its right to self-defense. Articles from Sputnik in 2023 and 2024 stress that Iranian officials such as Mansuri are unjustly framed as cyber aggressors, attributing their cyber activities to a necessity created by continuous Western cyber offensives and sanctions against Iran.

In several reports, Sputnik emphasizes that sanctions imposed on Mansuri and his colleagues are part of a larger geopolitical strategy aimed at containing Iran's technological

advancements. An article from early 2024 on Sputnik Iran mentions the implications of U.S. Treasury sanctions against IRGC cyber personnel, denouncing them as an attempt to undermine Iran's legitimate cybersecurity efforts. Sputnik further argues that sanctions contribute to destabilizing the region by penalizing Iran's self-protective cyber measures

Framing of Defensive Cyber Operations

Both Khabar Online and Sputnik Iran repeatedly frame cyber operations led by Mansuri as part of Iran's broader defensive strategy, positioning his actions within a narrative of state resilience and resistance to foreign exploitation. Iranian and sympathetic foreign outlets depict the focus on critical infrastructure security and information security measures as being consistent with global standards of sovereign defense. This portrayal seeks to counteract Western narratives of aggression by underlining Iran's stance on protecting its own digital borders.

Hamid Reza Lashgarian

Both Khabar Online and Sputnik Iran have focused on Hamid Reza Lashgarian's position as the head of the IRGC Cyber-Electronic Command, framing his role as one aligned with preserving Iran's cybersecurity sovereignty. In numerous articles, particularly those published after sanctions announcements, Iranian media defends Lashgarian by characterizing his activities as efforts to deter foreign interference in Iran's critical infrastructure. Khabar Online, in a 2024 piece, argues that Lashgarian's measures, which include overseeing cybersecurity measures across national infrastructure, represent a legitimate response to "foreign cyber aggression."

Mohammad Bagher Shirinkar

Shirinkar's activities are described by these outlets as part of Iran's broader strategy to counteract international cyber threats. Sputnik Iran frequently mentions his involvement in projects designed to bolster Iran's cyber defenses. In 2023, several Sputnik articles emphasized his role as a security leader ensuring that Iran's critical industries, such as water and energy, remain secure amid rising cyber threats from adversaries. The outlet dismisses claims that Shirinkar's operations are aimed at disrupting other nations' infrastructure, stating instead that his work centers on defensive protocols and innovations in cybersecurity.

Narrative Framing in Iranian Media

Across both outlets, the portrayal of IRGC cyber officials adheres to a consistent narrative of defense and resilience. Iranian reports argue that these figures act to neutralize cyber threats posed by U.S. and Israeli intelligence, often framing sanctions as part of a larger

political agenda. Coverage emphasizes that Iranian cyber activities, as directed by figures like Mansuri, Lashgarian, and Shirinkar, safeguard Iran's technological sovereignty, suggesting that Western objections are aimed at constraining Iran's advancement in cyber capabilities.

The defensive framing in Khabar Online and Sputnik Iran emphasizes that figures like Mansuri and Shirinkar are part of a necessary infrastructure to protect against increasingly sophisticated cyber tactics from foreign actors. These outlets reinforce that IRGC-CEC's activities are misrepresented by Western narratives and that Iranian cyber officials fulfill roles crucial to Iran's national security strategy.

CyberAv3ngers is a cyber threat actor group aligned with Iran's Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC). This group focuses on attacks targeting critical infrastructure, with operations involving industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, especially those related to water and wastewater facilities. Their online presence spans various platforms, including both mainstream social media sites and encrypted messaging apps, which they use to promote their agenda, share propaganda, and organize attacks. A deep dive into their online activities reveals a complex network that employs social media for both operational and influence-driven purposes.

Overview of CyberAv3ngers' Online Operations

CyberAv3ngers maintains a presence on several social media platforms, encrypted messaging apps, and lesser-known sites, using these channels to coordinate their activities and disseminate their messages. They use platforms like Telegram for communication, encrypted messaging, and sharing operational updates. Twitter, TikTok, and other social platforms often feature propaganda, claims of responsibility, and messages intended to intimidate adversaries. They also employ the Internet Archive to preserve records of their digital activities, allowing followers and potential recruits to access past content that may have been removed from mainstream sites.

Telegram: The Hub of Operations

Telegram remains the central platform for CyberAv3ngers, providing them with encrypted communication and the ability to create both public and private channels. The group operates a primary Telegram channel (https://t.me/CyberAv3ngers), where they share updates about their cyber activities, including claims of successful attacks on U.S. and Israeli infrastructure. They use this channel to post screenshots of compromised systems, share anti-Western rhetoric, and communicate with sympathizers. Additionally, they run several backup channels to ensure continuity if one is shut down. These backup channels

often feature similar content, ensuring their messaging reaches their audience despite potential disruptions.

CyberAv3ngers' Telegram account reveals an aggressive approach to both cyber operations and messaging, targeting equipment associated with Israel and sending provocations aimed at Israeli and U.S. infrastructure. The tone is taunting and confrontational, frequently casting their cyber activities as a direct challenge to Western cyber defenses. Each message often leverages clear, symbolic language intended to project confidence and provoke unease among targets.

On **November 28, 2023**, the group set a clear line of attack by declaring, “Every Equipment 'Made In Israel' Is Cyber Av3ngers Legal Target!” This stance reflects their intent to focus attacks on systems with Israeli origins, particularly ICS and SCADA systems frequently used in U.S. water and infrastructure facilities. This strategy targets specific components tied to national identities, amplifying the geopolitical tension behind each attack.

By **June 3, 2024**, CyberAv3ngers escalated their rhetoric, posting: “it's time to play some water 💧.” This statement implies an impending operation focused on water infrastructure, possibly targeting vulnerable systems in the U.S. or other regions where Israeli-manufactured PLCs and ICS components are utilized. Such posts serve as warnings that fuel tension and highlight their technical readiness for attacks that could disrupt essential services.

The post from **August 7, 2024**, “Have we been identified? Good Night TelAviv,” conveys a taunt directed at Israeli intelligence or cybersecurity authorities, suggesting that despite increased scrutiny, CyberAv3ngers maintains an upper hand or has evaded identification. By specifically mentioning Tel Aviv, they signal a threat that is both geographic and psychological, aimed at instilling fear of immediate or potential action against Israeli targets.

On **August 14, 2024**, CyberAv3ngers issued a clarifying statement about the existence of a fake channel impersonating them, followed by a message on **October 1, 2024**, stating that the fake channel had been reported to Telegram. This indicates that their identity and messaging are important to them, and they work to control their image and credibility within their follower network. It also demonstrates awareness of the risks posed by impersonators who might dilute or misrepresent their operations.

The message on **October 4, 2024**, takes a direct stance against cybersecurity agencies, specifically mentioning the FBI: “Check your systems and read our

message in the Alarm section. The message is clear: If you cyber bully, you will suffer irreparable damage before you have a chance to defend yourself. Oh, we're hiding behind our keyboards because the fbi has found out." This statement taunts law enforcement, warning of retaliation if CyberAv3ngers is targeted. The language emphasizes their confidence in remaining undetected and suggests that their methods are sophisticated enough to pose a significant threat even under active investigation.

Each of these messages reflects CyberAv3ngers' emphasis on control and intimidation, presenting their actions as a form of digital warfare with symbolic undertones aimed at both specific geopolitical opponents and broader cyber defense communities. Their Telegram presence creates a narrative of bold defiance and readiness to escalate cyber conflicts in highly targeted ways. Through these calculated announcements, CyberAv3ngers establishes an image of resilience and capability that aligns with Iran's broader goals in the cyber sphere.

Twitter and Archived Activity

Before being removed, CyberAv3ngers maintained an active presence on Twitter, using the platform to amplify their messages to a global audience. Their account, archived at https://web.archive.org/web/2/https://twitter.com/CyberAv3ngers, served as a space to post announcements of upcoming cyber operations, highlight their ideological stance, and react to geopolitical events. Twitter enabled them to engage with a broader, non-technical audience, allowing them to spread their messages and gain visibility beyond the closed circles of Telegram. Even after being banned from Twitter, their past posts and interactions remain accessible through the Internet Archive, reflecting their continued strategic use of accessible archives to preserve their narrative.

TikTok: Reaching a Younger Audience

CyberAv3ngers has adapted to platforms like TikTok (https://www.tiktok.com/@CyberAv3ngers?lang=en) to reach younger audiences. While TikTok may seem unconventional for a cyber group, they use the platform to disseminate short, provocative videos that combine footage of their cyber activities with nationalist and anti-Western themes. These videos often feature edited clips that mix defacement images from their hacks with music and patriotic messaging, aiming to appeal to younger users who may sympathize with their message. The short format of TikTok enables them to quickly communicate their claims and build a narrative around their supposed successes in disrupting adversary operations.

Internet Archive: Preserving Their Digital Footprint

CyberAv3ngers uses the Internet Archive (https://archive.org/search.php?query=CyberAv3ngers) to store content that may be removed from other platforms. They archive screenshots of their attacks, propaganda videos, and text-based declarations of their operations. This method allows them to bypass platform moderation and maintain a persistent digital footprint. Their archived content serves as a library of their activities, which can be accessed by followers or researchers even after original posts are taken down from mainstream sites. The Internet Archive's availability ensures that CyberAv3ngers' operational history remains accessible, supporting their efforts to claim legitimacy and document their cyber activities.

NSFW Content on ManyVids: An Unusual Twist

An unusual aspect of their online footprint is the presence of search results on adult content platforms like ManyVids (https://www.manyvids.com/results.php?keywords=CyberAv3ngers). While there is no clear indication that CyberAv3ngers themselves directly upload content here, it raises the possibility of their name being used or referenced in non-traditional online spaces. This could be a form of indirect propaganda or the result of adversaries or sympathizers co-opting their brand in unrelated contexts. Such occurrences highlight the challenges of tracking the true extent of their digital influence.

Coordination and Influence Campaigns

CyberAv3ngers employs these platforms not only for direct operational purposes but also as part of broader influence campaigns. They often share anti-Western narratives, criticizing sanctions and international policies that target Iran. Their messaging emphasizes resistance against Western powers, presenting their actions as a form of digital defense or retaliation against perceived aggression. They appeal to a sense of national pride among Iranian and pro-Iranian audiences, blending themes of technological empowerment with narratives of geopolitical struggle.

Their online activities align with broader Iranian state-sponsored narratives, suggesting coordination or at least alignment with Iran's strategic objectives. Reports and analysis from platforms like Voice of America (VOA) and other monitoring entities have observed how CyberAv3ngers' rhetoric matches that of Iranian state media, echoing the same themes of resistance and defense against external threats

Strategic Use of Encrypted Messaging

Encrypted messaging platforms, particularly Telegram, provide CyberAv3ngers with the ability to coordinate actions in a more secure environment. They use private Telegram groups to share tools, discuss tactics, and coordinate the timing of their attacks. These

private channels are less accessible to external monitoring, making them ideal for sensitive communications. CyberAv3ngers' use of Telegram reflects a broader trend among cyber groups to prioritize secure communication methods that reduce the risk of interception by foreign intelligence services.

Regional Influence and Impact

CyberAv3ngers directs its messaging to audiences in the Middle East, often referencing regional conflicts and portraying their cyber activities as part of a larger struggle against Western and Israeli influence. Their content often emphasizes the symbolic importance of their attacks on infrastructure, presenting each operation as a victory in a broader ideological conflict. This messaging finds a receptive audience among groups that support Iranian geopolitical goals or oppose Western involvement in regional affairs.

Their operations, however, extend beyond simple messaging. Reports of CyberAv3ngers' activities have included attempts to disrupt water facilities in the United States, specifically targeting control systems used in critical sectors

Their methods include spear-phishing, custom malware, and exploiting known vulnerabilities in outdated software, aiming to inflict operational damage while also broadcasting their technical prowess.

Summary Table: CyberAv3ngers Online Presence

Platform	Usage	Type of Content	Link/Reference
Telegram	Encrypted communication, propaganda, operational updates	Claims of attacks, screenshots, anti-Western messaging	https://t.me/CyberAv3ngers
Twitter (Archived)	Public declarations, propaganda, engagement	Announcements, anti-U.S. rhetoric, calls for support	https://web.archive.org/web/2/https://twitter.com/CyberAv3ngers
TikTok	Outreach to younger audiences	Short videos featuring defacements, nationalistic themes	https://www.tiktok.com/@CyberAv3ngers?lang=en
Internet Archive	Long-term content storage	Archived screenshots, operational records, propaganda material	https://archive.org/search.php?query=CyberAv3ngers

Platform	Usage	Type of Content	Link/Reference
ManyVids	Indirect references or unexpected associations	Unclear, potentially co-opted by third parties	https://www.manyvids.com/results.php?keywords=CyberAv3ngers

CyberAv3ngers' online activities reflect a sophisticated use of digital platforms for both operational coordination and influence operations. Their strategic use of mainstream and encrypted channels ensures their message reaches diverse audiences while maintaining a degree of operational security. The group's ability to adapt to platform restrictions and archive their content reflects a commitment to preserving their narrative and maintaining influence over their audience. Through platforms like Telegram and TikTok, they engage a variety of demographics, blending technical skill with a message of resistance against Western influence. Their digital footprint presents a challenge to global cybersecurity efforts, as it blends overt messaging with covert operational planning, making them a persistent presence in the cyber domain.

CyberAv3ngers and Soldiers of Solomon, both associated with Iran's Islamic Revolutionary Guard Corps (IRGC), often collaborate in cyber campaigns targeting critical infrastructure, especially in the U.S. and Israel. Operating under distinct but coordinated roles, they have worked together on high-profile campaigns, notably those targeting industrial control systems (ICS) and programmable logic controllers (PLCs) in water and energy sectors. Their operations gained traction in 2023, specifically around exploiting vulnerabilities in Unitronics PLCs, which are widely used in water and wastewater systems. These PLCs were targeted due to their Israeli manufacturing origin, a point CyberAv3ngers frequently highlighted in their anti-Israel messaging.

Organizational and Operational Structure

CyberAv3ngers, the primary actor group, takes on direct cyber actions like hacking, defacement, and network disruptions. According to reports from CISA, the FBI, and other agencies, CyberAv3ngers compromised Unitronics Vision Series PLCs using default passwords, publicly accessible internet connections, and weak configurations. They left defacement messages on ICS interfaces, such as "You have been hacked, down with Israel," signaling both a disruption of operational functionality and a clear political message

Soldiers of Solomon, another IRGC-affiliated group, focuses on supplementary cyber-intelligence operations and amplifies propaganda. Soldiers of Solomon often claim responsibility for the same attacks in which CyberAv3ngers are implicated, sometimes

exaggerating the scale of the intrusions. During an attack in October 2023, they alleged control over 50 servers, security cameras, and smart city management systems in Israel, though these claims were later verified as exaggerated by joint reports from U.S. and Israeli agencies

Social Media and Public Channels

CyberAv3ngers and Soldiers of Solomon disseminate their activities primarily through Telegram, Twitter (often archived), and a range of other niche platforms. Their **Telegram channels** provide a mix of verified posts and inflated claims, combining operational announcements with memes, threats, and propaganda. In posts, CyberAv3ngers have declared all equipment "made in Israel" as a legal target, further intensifying anti-Israel sentiments. Similarly, their cryptic messages, such as "Good Night TelAviv" following an attack, seek to generate fear and provoke responses from Israeli and U.S. authorities.

On **Twitter**, archived content shows both groups sharing politically charged statements and referencing cyber incidents aimed at entities using Israeli technology. Although Twitter's enforcement often leads to quick suspensions, the archived posts document their messaging history and interaction with followers.

In less conventional platforms like **Internet Archive**, they attempt to host mirrored content that links to Telegram or other underground channels. Here, the groups often post tactical guides, discuss vulnerabilities in SCADA systems, or share references to exploits they claim to have developed.

Campaigns and Tactical Methods

Targeting of Unitronics Devices

A focal point of CyberAv3ngers' campaigns involved the targeting of Unitronics PLCs due to their prevalence in water treatment and infrastructure facilities. Soldiers of Solomon supported these campaigns by amplifying claims of system takeovers, which were typically verified as overstated. The **Aliquippa, Pennsylvania** water facility incident became a case in point, where CyberAv3ngers temporarily manipulated water pressure controls, displaying a message on the interface accusing Israel, and briefly hijacked local management. Although mitigated swiftly, the incident underscored the risks posed by such IRGC-coordinated cyber attacks

"Crucio" Ransomware and Defacement Attacks

CyberAv3ngers deployed ransomware, notably "Crucio," in attempts to lock system access and demand political rather than monetary ransom. The malware, known for its straightforward deployment, was used to lock and manipulate ICS interfaces. In multiple

instances, Soldiers of Solomon exaggerated the success of these attacks, inflating narratives around damage levels and system control to bolster their propaganda and fuel anti-Israel rhetoric

Escalating Influence Operations

Beyond technical attacks, Soldiers of Solomon amplifies CyberAv3ngers' cyber actions with influence campaigns. Their posts frequently appear on **niche forums and obscure video-sharing sites** to target sympathizers and stir anti-Western sentiments. With text and visual propaganda, Soldiers of Solomon frames CyberAv3ngers' actions as defensive measures against Western cyber hegemony, often receiving support from outlets like Khabar Online and Sputnik Iran. These platforms reiterate claims of Western bias and cast IRGC's cyber efforts as necessary responses to perceived threats against Iran's sovereignty

Mitigation Responses and Security Recommendations

In response to CyberAv3ngers' actions, cybersecurity agencies in the U.S. and Israel have advised critical infrastructure organizations to strengthen security on ICS and SCADA systems. Recommendations include changing default PLC passwords, implementing multifactor authentication, disconnecting from public internet, and applying regular updates. The combination of cybersecurity hardening and public awareness campaigns seeks to limit the exposure of vulnerable industrial systems, mitigating the reach and effectiveness of CyberAv3ngers and Soldiers of Solomon

CyberAv3ngers, a cyber-actor group affiliated with Iran's Islamic Revolutionary Guard Corps (IRGC), reportedly uses OpenAI models as part of its research into programmable logic controllers (PLCs). By leveraging advanced AI tools, the group expands its technical knowledge of industrial systems, enabling more sophisticated cyber operations targeting critical infrastructure in the United States and Israel.

How CyberAv3ngers Uses AI in Cyber Research and Attack Planning

1. **Research on Programmable Logic Controllers (PLCs)**
   PLCs are specialized devices integral to the automation and control of infrastructure systems, including water treatment plants, power grids, and manufacturing facilities. PLCs manage functions ranging from temperature control to pressure regulation and are crucial in maintaining operational stability. CyberAv3ngers has conducted extensive research on PLCs with the intent to identify vulnerabilities within these systems. Using AI tools, the group can analyze complex system configurations, identify potential attack vectors, and simulate access methods for PLCs. OpenAI models enable rapid research by processing vast amounts of data on PLC architectures, vulnerabilities, and possible exploit strategies.

2. **Exploit Development and Vulnerability Analysis**
   AI language models can aid in understanding technical documentation, researching specific PLC models, and developing potential exploit frameworks. By accessing AI-driven insights, CyberAv3ngers might efficiently discover or replicate known weaknesses in PLC systems and adapt them into malware or custom code designed to interfere with infrastructure operations. For example, using AI to translate or interpret complex technical documents on PLC configurations allows CyberAv3ngers to identify possible weak points that may otherwise require a highly skilled engineer to discover.

3. **Testing and Simulating Attack Scenarios**
   AI models help simulate cyber-attack scenarios, enabling CyberAv3ngers to test different methods of intrusion and control. By using AI tools to model how a PLC would respond to certain inputs or malicious commands, the group can refine its tactics without immediate access to live industrial systems. These simulations help in crafting attacks that are more likely to succeed in the field, while reducing the trial-and-error traditionally required to compromise such specialized equipment.

4. **Targeting Critical Infrastructure in the U.S. and Israel**
   CyberAv3ngers has concentrated its cyber operations on critical infrastructure in the United States and Israel, focusing on systems using Israeli-manufactured PLCs. OpenAI models can enhance the group's ability to conduct reconnaissance on these targets, understanding the structure of U.S. and Israeli industrial systems to better pinpoint vulnerabilities. Reports indicate that the group's recent campaigns have included efforts to disrupt water and energy services by manipulating PLC-controlled elements, with attack methodologies evolving to exploit newly identified weaknesses.

Strategic Implications of AI-Assisted Cyber Operations

CyberAv3ngers' application of AI to industrial control systems represents a significant evolution in cyber warfare, as AI models can streamline complex research and lower the skill threshold required for highly technical attacks. Traditional cyber campaigns against PLCs and ICS components require considerable technical knowledge, but AI can democratize access to such expertise. This development poses an emerging threat to critical infrastructure worldwide, as malicious actors can now perform high-level research and operational planning without needing to source specialized human expertise.

CyberAv3ngers' utilization of OpenAI models in researching PLCs for cyber operations underscores a trend where advanced AI tools facilitate more efficient, lower-cost cyber

warfare. By effectively harnessing AI, CyberAv3ngers gains an edge in identifying, testing, and deploying attacks against critical infrastructure, expanding the IRGC's reach and capabilities in cyberspace. Their focus on U.S. and Israeli targets illustrates the strategic goals underpinning these operations, while also highlighting the urgent need for countermeasures that can defend against AI-augmented cyber threats.

CyberAv3ngers has demonstrated a distinctive, structured approach that aligns with tactics frequently associated with nation-state-backed groups, despite its categorization as a hacktivist group rather than a full advanced persistent threat (APT). Their **modus operandi** reflects a focused strategy on vulnerable, internet-connected operational technology (OT) in critical infrastructure—especially programmable logic controllers (PLCs) from the Israeli manufacturer Unitronics. This analysis yields new insights into CyberAv3ngers' evolving capabilities, underlying tactics, and potential vulnerabilities.

1. Strategic Focus on Specific PLCs and ICS Targets

CyberAv3ngers' persistent targeting of Unitronics PLCs, particularly in the U.S. water infrastructure, suggests a tactical fixation rather than a broad capability to compromise multiple industrial control systems (ICS) brands. Their reliance on attacking devices with default settings, such as open internet-facing ports and factory-default passwords, points to a methodological limitation, as well as a high dependency on unpatched systems with easily exploited configurations. This narrow focus may be a deliberate choice, allowing them to develop repeatable attack tactics against a single platform, which could then be adapted for use against similar models or infrastructure. However, it also suggests that their reach may be limited if defenders secure these PLCs following recommended hardening practices.

2. Operational Tactics Using Basic but Effective Methods

CyberAv3ngers uses low-complexity, high-impact tactics—such as brute-forcing credentials or taking advantage of unsecured credentials—which enables rapid compromises without requiring advanced technical skill. Their methodology reflects a pragmatic approach often used by hacktivist movements with limited resources or specialized training. This tactic is amplified through symbolic gestures, including defacement messages that send political statements, and deliberate target choices that reinforce their anti-Israel and anti-Western narratives.

The group's activities frequently culminate in **defacement and data leakage**, both of which serve dual purposes: disrupting operations and amplifying the psychological impact of the attack. The messages left on hacked systems are often politically charged, targeting

Israeli-made components or infrastructure with ties to political adversaries, further reinforcing the hacktivist nature of CyberAv3ngers' campaigns.

3. Role of Soldiers of Solomon as a Supporting Propaganda Arm

The group known as **Soldiers of Solomon**, linked to CyberAv3ngers, plays a complementary role, amplifying CyberAv3ngers' successes and making exaggerated claims. In one instance, Soldiers of Solomon alleged they had seized control over 50 Israeli servers, though these statements were not fully substantiated. This exaggeration contributes to a narrative of cyber dominance, bolstering the perceived threat while likely overplaying actual successes. Soldiers of Solomon also serves as a distribution arm for propaganda, leveraging various media outlets to communicate CyberAv3ngers' political message and intensify its impact across sympathetic communities and social networks.

4. Dependence on Public Channels and Minimal Stealth Tactics

CyberAv3ngers operates openly on **Telegram**, **Twitter**, and various internet archives, favoring public visibility over stealth. Their communications strategy is unambiguous, often issuing warnings prior to attacks or taunting adversaries afterward. While this approach enhances their visibility, it contrasts with the covert methods employed by traditional APT groups, who prioritize stealth to maximize the impact of cyber-espionage or cyber-sabotage efforts.

Open channels allow CyberAv3ngers to broadcast threats and claim responsibility, reinforcing their political stance and appealing to their support base. However, the open nature of their communications also makes them susceptible to intelligence tracking, providing a trail that security agencies can follow. By openly acknowledging the Soldiers of Solomon as affiliates, CyberAv3ngers risks associating themselves with propaganda campaigns that may undermine their credibility.

5. Emergence of Crucio Ransomware as a New Operational Tool

CyberAv3ngers' acquisition and customization of Crucio ransomware indicate a shift toward financially motivated disruption. Ransomware allows them to compromise and control infrastructure at a more granular level, elevating the potential for damaging attacks that lock out operators from essential services. The **Crucio ransomware** variant reportedly includes remote capabilities for data encryption and partial destruction, providing the group with an additional layer of threat beyond defacement or data theft.

However, CyberAv3ngers has not demonstrated the same adaptability or flexibility in ransomware deployment seen in other groups, indicating that they may still be in the

testing phases. Their focus remains on ICS and PLC systems with established vulnerabilities rather than attempting novel exploits or zero-day attacks.

6. Intelligence Implications and Opportunities for Countermeasures

CyberAv3ngers' repetitive targeting of exposed PLCs and reliance on social media for communication offer several exploitable vulnerabilities. Enhanced monitoring of open-source intelligence, social media, and internet archive activity could yield actionable intelligence on their planned operations. Their willingness to broadcast targeting priorities—such as "Every Equipment 'Made In Israel' Is Cyber Av3ngers Legal Target!"—suggests predictable attack patterns that defenders can anticipate.

CyberAv3ngers exemplifies a state-sponsored hacktivist group with a focused, low-complexity approach to cyber operations. By repeatedly targeting Unitronics PLCs and similar ICS components, they exploit predictable vulnerabilities to impact high-value infrastructure in the U.S. and Israel. Their continued evolution, marked by the integration of ransomware like Crucio and a partnership with Soldiers of Solomon, highlights the IRGC's effort to weaponize hacktivist groups as disruptive cyber entities. CyberAv3ngers' visibility and specific targeting patterns present unique counterintelligence opportunities, allowing defenders to develop tailored strategies that anticipate and mitigate their disruptive operations.

The CyberAv3ngers—a group thought to be a blend of Iranian state-backed and proxy-affiliated hackers—are likely to target sectors and regions tied to Iran's strategic goals, particularly where they can exploit vulnerabilities and incite geopolitical reactions. Here are the anticipated next moves and tactics:

1. **Targeting U.S. and Allied Critical Infrastructure**:
    - **Energy and Financial Sectors**: Given previous Iranian APT focus on these sectors, CyberAv3ngers may aim at critical infrastructure in the U.S., Europe, or the Gulf states. This could involve ransomware or wiper malware against energy grids, oil facilities, and financial networks, aimed at disrupting or pressuring regional competitors and allies of the U.S..
    - **Healthcare and Defense Contractors**: Expanding into healthcare and contractors linked to U.S. defense, CyberAv3ngers may deploy spear-phishing or supply chain attacks to access sensitive data, disrupt services, or gain leverage in international negotiations.
2. **Social Media Manipulation and Influence Operations**:

- **Psychological Warfare and Social Disruption**: CyberAv3ngers are expected to leverage influence operations via social media platforms, particularly around sensitive U.S. domestic issues (e.g., racial justice or electoral debates), similar to tactics observed in prior Iranian influence campaigns targeting U.S. social movements.
- **Fabricating or Amplifying "Counter Narratives"**: They may use AI-enhanced deepfake videos or compromised social media accounts to manipulate public sentiment. In these cases, tactics could include impersonating high-profile individuals or deploying bots to promote divisive hashtags, potentially swaying public opinion around Iranian or regional issues.

3. **Enhanced Retaliatory and Proportional Cyber Attacks**:
   - **Proportional Retaliation Strategy**: Iran's desire for "proportional" retaliation could see CyberAv3ngers conducting sophisticated cyber operations on par with recent attacks that Iran has faced. This might involve precision attacks on high-profile institutions in Israel, Saudi Arabia, or Europe, which can serve both retaliation and strategic disruption purposes.
   - **More Focused Cyber-Espionage**: Iran may direct CyberAv3ngers to use espionage for collecting intelligence on U.S. or EU policies impacting Iran, especially concerning sanctions or military operations in the region. This could manifest as surveillance-oriented attacks on Western government entities and NGOs.
4. **Hybrid Tactics and Multi-Vector Operations**:
   - **Converging Cyber and Physical Influence**: CyberAv3ngers may coordinate cyber-attacks with physical and online influence tactics across the Middle East, using digital disruptions to support or conceal on-ground proxy actions. This tactic has been used to assist IRGC-backed proxies in regions such as Iraq and Syria.
   - **Testing AI for Phishing and Brute Force Attacks**: Recent reports suggest that Iranian cyber actors may employ AI-based phishing techniques to improve their attack success rates, particularly against targets like government and military contractors in Western nations.

Overall, CyberAv3ngers are likely to continue evolving their methods with increasing complexity, blending sophisticated hacking, deepfake influence, and careful selection of

targets to maximize psychological and economic impact, especially within U.S. and allied nations.

1. ** Known for cyber and propaganda operations, Soldiers of Solomon appear to function as a proxy for the IRGC in psychological and influence warfare. Using social media, they amplify narratives that counter anti-regime sentiments, often targeting Western audiences or dissident groups within Iran. Their activities align closely with IRGC goals and methods, blending cyber tools with ideological influence to destabilize opposition .

2. **0ktapus**: Operatimilar tactics as Iran's established cyber groups, 0ktapus is known for its technical sophistication, particularly in credential harvesting and data exfiltration from compromised systems. They utilize spear-phishing and social engineering, making them a valuable tool in the IRGC's arsenal against targets of geopolitical interest, often aligned with regional adversaries .

Prominent Threats and Technique Rhysida ransomware is often deployed in conjunction with other malware or spear-phishing attacks. It is designed to encrypt data and disrupt systems, targeting both government and private sector organizations critical to infrastructure. Its tactical application reflects Iran's penchant for economic and psychological warfare—weakening adversaries through financial strain and operational paralysis .

2. **Crucio**: Crucio represents a multi-phase malwaactic favored by groups like MuddyWater and Static Kitten, both affiliated with Iranian operations. Crucio's adaptability allows it to collect data from a broad range of sectors, including telecommunications, academia, and NGOs, aligning with the broader Iranian objective of intelligence collection. Its deployment often coincides with geopolitical events, used strategically to leverage Iran's information-gathering or retaliatory aims 【32†source】.

Integrated Strategic Objectives and Methods

Iranider the IRGC employ a multi-layered approach that combines these actors and threats:

1. **Hybrid Warfare**: These groups operate under a hybrid model, integrating cyber threats (e.g., malware and ransomware) with social media influence to create confusion, amplify propaganda, and suppress dissent. By deploying groups like CyberAv3ngers and Soldiers of Solomon, Iran expands its reach to destabilize public opinion, both domestically and internationally 【37†source】.

2. **Data and Credential Theft**: Many of these campaigns (e.on extracting credentials and sensitive data, which are then used for long-term espionage or to compromise additional targets. The IRGC often weaponizes this information to pressure foreign governments or intimidate individuals within hostile regions .
3. **Geopolitical Influence**: The IRGC's collaboration with entities like CyberAnd technical attacks to influence campaigns. By leveraging Crucio or Rhysida alongside disinformation tactics, the IRGC destabilizes rival states, aligning with its broader geopolitical mission to reduce Western influence in the region .

These Iranian-aligned actors and threats, coordinated chiefly by the IRGC, present a comprehensive and cyber threat landscape. Through combining technical attacks with influence operations, they aim to achieve both tactical and ideological goals, targeting critical infrastructure, political figures, and opposition voices alike.