Between Tehran and Tirana

Shaul Shay

(Senior research fellow at the International Institute for Counterterrorism (ICT) at the Interdisciplinary Center Herzliya and former deputy head of Israel's National Security Council)

Albanian Prime Minister, Edi Rama, arrived in Israel on October 23, 2022 for a three-day visit to seek protection from Iranian cyberattacks. Prime Minister Rama's visit came a month after Albania cut diplomatic ties with the Islamic Republic after a series of cyberattacks it attributes to Iran. Rama's delegation includes Albania's cyber director and the national security adviser and chief spokesperson.

After Albania cut diplomatic ties with Iran, a second cyberattack from the same Iranian source hit an information system - the Total Information Management System (TIMS), a system that records Albanian border entries and exits.

Israeli Prime Minister, Yair Lapid said: "Iran represents a joint threat for Israel and Albania, and we saw this in the recent Iranian cyberattacks against Albania. Israel will assist in any way in the effort against Iran. We see this as a national interest and a historical responsibility."[1]

Israel offered cyber defense assistance to Albania days after it severed its diplomatic ties with Iran. Deputy Foreign Minister, Idan Roll, met with Albanian Foreign Minister Olta Xhacka on the sidelines of the Conference in Berlin, where he "offered to share our knowledge and experience in cyber defense" and "expressed Israel's appreciation" for Tirana's decision to kick out Iran's diplomats.[2]

Israel and Iran have for several years been involved in a largely clandestine cyberwar. In 2020, Iran-backed hackers reportedly attempted to attack and sabotage Israeli water and sewage facilities. Attacks attributed to Iran-backed hackers have also targeted medical facilities in Israel.[3]

Iran and Albania have been bitter foes for years, since Albania began hosting members of the Iranian opposition Mujahedeen-e-Khalq (MEK), on its soil through an arrangement between the U.S. and Albania.

In the course of more than 40 years Iran is the world's leading state sponsor of terrorism. Iran has objected to Albania's hosting of MEK members, saying its national security is being threatened and is operating against both the MEK and Albania:

Cyber-attacks against Albania and the MEK.

Terror threats against MEK on Albanian soil and beyond.

Political pressure on Albania.

In an interview to the Washington Post Albanian Prime Minister explained why he cut diplomatic ties with Iran after cyberattack: "It's practically bombing the country you know, destroying critical infrastructure," Rama said of Iran's attacks. "The bombs are not visible, the wounds are not physical, thank God, but still [it] is an aggression, a bombardment, and its direct harm to the national sovereignty. … Would you keep the country that bombards you?"[4]

The Mujahideen-e-Khalq (MEK)

The People's Mujahideen Organization of Iran (PMOI), also known by its Farsi name Mujahideen-e-Khalq (MEK), was formed in the 1960s by Marxist-Islamist urban guerrillas opposed the rule of Shah Mohammad Reza Pahlavi. In the 1970s the MEK carried out terror attacks against the Iranian shah's government and its American allies.

Later MEK participated in the 1979 Iranian Revolution but soon it had a falling out with Ayatollah Ruhollah Khomeini and embarked on a decades-long campaign to overthrow the Islamic regime. The MEK fled into Iraq and backed Saddam Hussein during his eight-year war with Iran in the 1980s and violently opposed the Islamic Republic from Iraqi territory.

The United States designated MEK as a terrorist organization in 1997 and after the overthrow of Saddam Hussein by the U.S.-led coalition in 2003, the MEK in Iraq was disarmed and thousands of its members isolated at Camp Ashraf, near the Iranian border in eastern Iraq, as "protected persons" under the Geneva conventions.

The U.S. removed its terrorist label from MEK in 2012, crediting the group's public re-annunciation of violence, the lack of any confirmed militant attacks by the group in more than a decade, and its cooperation in the closure of its paramilitary base in Iraq, from where its members relocated to Albania.

Albania has hosted MEK members since 2013 in Manez a town in Durres County and the location of a camp where about 3,000 MEK members are located. Although now largely based in Albania, the group claims to operate a network inside Iran.

The Iranian MEK is an opposition movement in exile, which wants to bring down the Islamic Republic of Iran. Led by Maryam Rajavi, the Iranian dissidents in exile cast themselves as an alternative to the Iranian regime.

Rajavi told Reuters in July 2019 she stood for democracy, separation of the state and religion, private investments and a non-nuclear Iran.[5]

The Iranian cyber-attacks against Albania

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a report to provide information on recent cyber operations against the Government of Albania in July and September 2022.[6]

In July 2022, Iranian state cyber actors—identifying as "Homeland Justice"—launched a destructive cyber-attack against the Government of Albania which rendered websites and services unavailable.

The preparations [7]

An FBI investigation indicates Iranian state cyber actors acquired initial access to the victim's network approximately 14 months before launching the destructive cyber-attack, which included a ransomware-style file encryptor and disk wiping malware.

The actors maintained continuous network access for approximately a year, periodically accessing and exfiltrating e-mail content.

Between May and June 2022, Iranian state cyber actors conducted lateral movements, network reconnaissance, and credential harvesting from Albanian government networks. In June 2022, Homeland Justice created a website and multiple social media profiles posting anti-MEK messages.

The first cyber-attack (July 15, 2022)

In July 2022, the actors launched ransomware on the networks, leaving an anti MEK message on desktops. When network defenders identified and began to respond to the ransomware activity, the cyber actors deployed a version of ZeroCleare destructive malware.[8]

Prime Minister Edi Rama accused Iran of directing a cyberattack against Albanian institutions on July 15, 2022, in a bid to "paralyze public services and hack data and electronic communications from the government systems". Prime Minister Rama added that "damages may be considered minimal compared to the goals of the aggressor. All systems came back fully operational and there was no irreversible wiping of data".[9]

On July 18, 2022, Homeland and Justice took credit for the cyber-attack on Albanian government infrastructure.

On July 23, 2022, Homeland Justice posted videos of the cyber-attack on their website. From late July to mid-August 2022, social media accounts associated with Homeland Justice demonstrated a repeated pattern of advertising Albanian Government information for release, posting a poll asking respondents to select the government information to be released by Homeland

Justice, and then releasing that information—either in a zip file or a video of a screen recording with the documents shown.[10]

The second cyber attack

On September 10, 2022, Iranian cyber actors launched another wave of cyber-attacks against the Government of Albania, using similar malware as the cyber-attacks in July 2022.

The country's interior ministry said the national police's computer systems were hit by a cyber-attack. According to a statement from Albania's interior ministry it forced Albanian officials to temporarily take offline its Total Information Management System (TIMS), a system for tracking the data of those entering and leaving Albania.

The US government in 2007 helped Albania, an ally in the Bush administration's "war on terrorism," deploy the TIMS hardware and software systems for processing immigration.[11]

The Albanian response

Albania cut off diplomatic relations with Iran over the cyberattack that destroyed government data and shut down services. It was the first known time a nation has taken such an aggressive step in response to a cyberattack, and it generated support from several other nations, including the United State.[12]

Albanian Prime Minister Edi Rama said that the attack was "state aggression" that "threatened to paralyze public services, delete systems, and steal state data, steal electronic communications within the government system and fuel insecurity and chaos in the country." That forced Albania to take "extreme measures," he continued.

"The government has decided, with immediate effect, to end diplomatic relations with the Islamic Republic of Iran," Rama said. It also expelled Iranian Embassy staff.[13]

The Iranian diplomats were linked to Iran's Islamic Revolutionary Guard Corps (IRGC) and the ministry of intelligence. Both entities have been implicated in terror and assassination plots in Europe, targeting exiled opponents of the regime in Tehran.

The Iranian response

Iran rejected the accusation it was behind the cyberattacks as "baseless" and called Albania's decision to sever diplomatic ties "an ill-considered and shortsighted action."

"Iran as one of the target countries of cyberattacks on its critical infrastructure rejects and condemns any use of cyberspace as a tool to attack the critical infrastructure of other countries," its foreign ministry said.[14]

After diplomatic ties were severed over the cyberattacks, Iranian diplomats were reported to have burned papers inside the Iranian embassy in Tirana, which may indicate sensitive and intelligence documents were kept there.

On September 10, 2022, Iranian cyber actors launched another wave of cyber-attacks against the Government of Albania. These were likely done in retaliation for public attribution of the cyber-attacks in July and severed diplomatic ties between Albania and Iran.[15]

The U.S. and NATO response

The U.S. and NATO were quick to support Albania in reinforcing its cyber security.U.S. National Security Council spokesperson Adrienne Watson said American experts had concluded that Iran "conducted this reckless and irresponsible cyber-attack" and that it was "responsible for subsequent hack and leak operations".[16]

The United States said it strongly condemned the cyber-attack on a NATO ally and vowed to hold Iran accountable for actions that threatened Albania's security. The U.S. announced sanctions on Iran's Ministry of Intelligence and Security and its minister Esmail Khatib over Tehran's alleged involvement.

The Iranian terror threats

Iran has been chasing MEK members and other Iranian dissidents across continental Europe. General Yahya Rahim Safavi, the Supreme Leader's military advisor and former IRGC commander-in-chief warned that: "If necessary, the IRGC will hunt and crackdown on dissidents and enemies beyond borders and seas".

To carry out such terror operations, Iran uses a wide network of the IRGC's - al - Quds Force, the Ministry of Intelligence (MOIS) and proxies like Hezbollah. Iran also has an organized terrorist network established in Europe including in Albania.

In December 2018, the Iranian ambassador in Tirana and another diplomat were expelled over an alleged terrorist plot whose exact nature has not been made public.

On October 23, 2019, the Albanian State Police announced it had foiled attacks planned in 2018 by Iranian agents against MEK members living in Albania. The terrorist cell of the foreign operations unit of Police General Iranian QUDS planned to attack high-level MEK members attending Persian New Year festivities in March 2018 in Tirana but were prevented from doing so by Albanian police action. [17]

On July 23, 2020, a suspected agent sponsored by Iranian authorities was declared "unwanted" by the Government of Albania and subsequently expelled from the country.

In October 2020, Bijan Pooladrag, an Iranian citizen was arrested in Albania. He was suspected of working for the Iranian secret services and of eavesdropping on MEK.[18]

The " July 2022" Iranian terror plot

The MEK regularly hosts summits in Albania that have long attracted support from conservative U.S. Republicans, including former U.S. vice president Mike Pence, who delivered a keynote address at an event.

Iranian dissidents from the Mujahedeen-e-Khalq, (MEK) in Albania said on July 22, 2022, they had canceled a summit following warnings from local authorities of a possible terrorist threat.[19]

They had planned to hold the "Free Iran World Summit" on July 23-24,2022, with the participation of U.S. senators and congressmen and other former personalities from Western countries to "call on the Biden administration to adopt a decisive policy against the Tehran regime."

A statement from the MEK said the summit was "postponed until further notice upon recommendations by the Albanian government, for security reasons, and due to terrorist threats and conspiracies."[20]

The U.S. Embassy in Tirana warned its citizens that it was "aware of a potential threat targeting the Free Iran World Summit" calling on its citizens "to avoid this event."

The July 15, 2022, cyber-attack took place a week before the conference in Albania due to be attended by members of MEK.[21]

On July 16, 2022, the Albanian media reported that the country's Special Structure for Combatting Corruption and Organized Crime (SPAK) acting on the request of the Special Prosecutor's Office, detained and interrogated 20 Iranians for espionage in the service of the Iranian regime.[22]

Albanian Police raided eight apartments, four offices, and several buildings where they stayed and conducted prohibited activities.

According to the Albanian Police, these individuals had been under investigation for four years. They are suspected of carrying out espionage activities on Albanian territory on behalf of the Islamic Revolutionary Guards Corps (IRGC) and the Ministry of Intelligence and Security (MOIS).[23]

Political pressure on Albania - the "Qasem Soleimani affair

Following the escalation of tensions between the US and Iran after the killing of Iranian General Qassem Soleimani, the Supreme leader of Iran, Ali Khamenei, in a speech, on January 8, 2020, considered Albania a problematic European country that is giving shelter to the enemies of Iran.

"There is a small, devilish country in Europe where Americans are cooperating with Iranian traitors, plotting against the Islamic Republic. Their plan was clear, with the protests they held in Iran, since some of those traitors came to Iran to protest. Enemy agents started implementing a plan to sabotage and destroy our government and our Constitution", Ali-Khamenei declared.[24]

Albanian President Ilir Meta shot back at comments made by Ali Khamenei. He said that Albania is not a devilish country, but a democratic country that has suffered from an unprecedented devilish dictatorship and has come to value human rights as sacred.[25]

Summary

The relationships between Iran and Albania have gone bitter since 2013 when Albania began hosting more than 3000 members of the opposition People's Mujahedeen of Iran, or Mujahedeen-e-Khalq (MEK), on its soil.
Albania, a close U.S. ally has found itself on the frontline of the clash between the West and Iran and Albania has been at the center of terrorist activities and cyber-attacks organized by Iran, due to hosting the Mujahideen-e-Khalq (MEK).

The Iranian cyber-attacks on Albania came after Iran failed to convince Albania to remove the MEK members from its territory and after repeated attempts by Iran to carry out terror attacks against the MEK on the territory of Albania in the years 2018 - 2022 were thwarted.
This was not the first time that Iran combines terrorist attempts with cyber-attacks and they have often done so in other arenas such as against Israel, Saudi Arabia and more.

The latest Iranian cyber-attacks and terror plots in Europe are a warning and a wake-up call to governments in Europe to reexamine the appeasement polices toward the Iranian regime.

Notes:

[1] Lazar Berman, citing common threat from Iran, Lapid pledges cyber defense help to Albania, The times of Israel, October 23, 2022.

[2] Israel offers cyber aid to Albania, which severed Iran ties over hacking claim, the times of Israel, September 13, 2022.

[3] Tzvi Joffre, how is Albania's severance of ties with Iran related to Israel? The Jerusalem Post, September 7, 2022.

[4] Tim Starks, How Albania reckoned with alleged Iranian hackers, The Washington Post, September 26, 2022.

[5] Benet Koleka, Albania says it foiled Iranian plot to attack exiled dissidents, Swissinfo.ch, from October 23, 2019. Retrieved January 17, 2020.

[6] Iranian State Actors Conduct Cyber Operations Against the Government of Albania, the Cybersecurity and Infrastructure Security Agency (CISA), September 21, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-264a#:~:text=Cybersecurity%20and%20Infrastructure%20Security%20Agency%20(CISA)a.

[7] Ibid.

[8] Ibid.

[9] Albania Suffers 2nd Cyberattack, Blames Iran, VOA, September 10, 2022.

[10] Iranian State Actors Conduct Cyber Operations Against the Government of Albania, the Cybersecurity and Infrastructure Security Agency (CISA), September 21, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-264a#:~:text=Cybersecurity%20and%20Infrastructure%20Security%20Agency%20(CISA)a.

[11] Ibid.

[12] Tim Starks and Aaron Schaffer, Albania is the first known country to *sever diplomatic ties over a cyberattack*, The Washington Post, September 8, 2022.

[13] Ibid.

[14] Albania Suffers 2nd Cyberattack, Blames Iran, VOA, September 10, 2022.

[15] Iranian State Actors Conduct Cyber Operations Against the Government of Albania, the Cybersecurity and Infrastructure Security Agency (CISA), September 21, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-264a#:~:text=Cybersecurity%20and%20Infrastructure%20Security%20Agency%20(CISA)a.

[16] Gritten David, Albania severs diplomatic ties with Iran over cyber-attack, BBC News, September 7, 2022.

[17] Albania Police Expose 'Terrorist Cell' Targeting Iranian Exiles, BalkanInsight, October 23, 2019.

[18] Iranian Citizen Faces Terrorism Charges in Albania, Balkan Insight, April 1, 2022.

[19] Terror threat cancels Iranian opposition's summit in Albania, AP, July 22, 2022.

[20] Terror threat cancels Iranian opposition's summit in Albania, AP, July 22, 2022.

[21] Lyngaas Sean, Albania blames Iran for second cyberattack since July, CNN, September 12, 2022.

[22] Saed Abed, Police Operation Debunked MOIS Agents Disguised as Soia in Albania, Linkedin, August 16, 2022.

[23] Ibid.

[24] Iranian leader, Al-Khamenei, addressed to Albania as a 'small, diabolic country in Europe' Top channel tv, from January 8, 2020. Retrieved January 15, 2020.

[25] Gjergj Erebara, Albania Expels Two More Iranian Diplomats, Balkaninsight, from January 15, 2020. Retrieved January 18, 2020.