The Gaza war is only a part of Iran’s grand plan

written by Joseph Rozen | 04.12.2023

During a UN Security Council meeting on the 24th of October, the secretary general, Antonio Guterres, said that Hamas’ October 7th attacks on Israel “did not happen in a vacuum”. He was not wrong – Hamas’ attacks were planned and executed with the close assistance of Iran, which continues to arm, guide, finance, and activate its proxies in the Middle East.

The Israel-Gaza war has repercussions on the international fight against Iran and its other accomplices. Hezbollah in Lebanon, the Houthis in Yemen, and Shia militias in Syria, Iraq, and recently in Sudan, are all Iranian agents of chaos and terror, who serve Iran’s interests – to create a Shia-dominate strip stretching from Iran to the Mediterranean Sea to shift the leadership of the Muslim world from Sunni countries to Iran, end the US presence in the Middle East and destroy Israel. Besides Iranian direct support, the use of these proxies would not have been effective without an envelope-supporting system of private entities, with the ability to enable money transfers, technologies, communications, etc.

The current situation in the Middle East provides an opportunity to increase global efforts to stop Iran’s malign behavior, not only by sanctioning Iran and its proxies but also use complementary measures to sanctions and target private companies which assist Iran in executing terror activities.

The Military Sphere

After the fog of October 7th atrocities faded away, the Israeli defense forces were able to recover Iranian-produced weapons used by Hamas during the October 7th attack. The Foundation For Defense of Democracies (FDD) reported that 60mm mortar rounds with Iranian-made AZ111 mortar round fuses and M112 demolition charges were used by Hamas in the attack. Evidence shows that these components were produced in Iran and appear in a catalogue of the Defense Industries organization, an Iranian company that is affiliated with the Ministry of Defense of Iran. The M112 explosives recovered were identical to those intercepted by US-led operations in Yemen and Bahrain to stop smugglers.

In addition to these familiar weapons, the IDF has also recovered new Iranian-made warheads for Rocket-propelled grenade launchers (RPG) that were not seen before. In the new warhead, the first charge is designed to penetrate light armoured vehicles and the second charge is thermobaric, aimed at burning the target.

The latest launching of drones and cruise missiles by the Houthis in Yemen towards Israel demonstrated more Iranian weapons variety. Since November last year, the US Navy seized many weapons and munitions en route to Yemen, in the area of the Red Sea and Gulf of Aden. These included explosives, ammunition, weapons and missiles, which are in the use of Hamas and other proxies as well.

Iran's creativity goes as far as its cruelty in its efforts to maintain a flow of arms to Iranian proxies in the region. Following the devastating earthquakes that hit Syria in February 2023, the IRGC used humanitarian assistance as camouflage to transfer weapons and crucial components to assist with Hezbollah's efforts to turn their rockets more accurate. Recently, Syria accused Israel of launching simultaneous missile attacks against its airports, probably to stop the already known route of weapons transfer from Iran to Syria and further to Hezbollah. After the destruction of these airports, Russia hurried to allow Iranian flights to use the "Khmeimim" air base in Syria. This is happening while Hezbollah and Shia militias in Syria have been targeting Israel with rockets since October 7th.

The technological efforts

Alongside supplying weapons to terrorist organizations, Iran is also very active in the technological sphere, which is crucial for securing funds for terrorism, surveillance, and supporting other terror-related activities inside and outside Iran.

ArianTel, an Iranian wireless communications services provider was pivotal to Iran's efforts to create a large-scale surveillance network. According to Citizen Lab, a cybersecurity NGO based in Canada, the surveillance and censorship capabilities resulting from this level of integration with mobile service providers cannot be understated.

Prime example for this is MTN Group. MTN entered the Iranian telecom sector in 2005 and launched its services in Iran a year later using a subsidiary named Irancell, a front company of the IRGC, in which MTN owns a 49% stake, the other

51% owned by the Iranian Electronic Development Company. Since then, MTN has been closely involved with ArianTel, as part of its joint venture with the Iranian government. MTN and Irancell, provided multiple Access Points and Roaming agreements, granting ArianTel explicit access to their cellular networks. This allowed ArianTel and the Iranian government to carry out surveillance operations on dissidents and critics within Iran.

MTN group openly and knowingly conducted business with the IRGC and ArianTel despite international sanctions against them. In April 2023, ArianTel was sanctioned by the European Union, for contributing to the telecommunications surveillance architecture mapped out by the Iranian government to quash dissent and critical voices in Iran. In 2020, a year after IRGC was officially designated as a foreign terrorist organization (FTO) MTN released a statement saying that it would continue its business as usual.

MTN made conscious decisions to engage in misconduct while violating sanctions, and effectively supporting and facilitating Iran's terrorism. But the use of telecommunication systems does not stop at surveillance and suppressing dissent at home, rather it is used to advance Tehran's international aspirations as well, supporting Iran's proxies in Syria, Iraq, Lebanon, Gaza, and Yemen.

This activity is at the core of the US district court in New York's high-stakes anti-terrorism act lawsuit against MTN Group. In addition to its direct engagement with the IRGC, the lawsuit revealed the group's violations of the Anti-Terrorism Act by paying protection money of more than $100M to al-Qaeda and the Taliban so they wouldn't target its cellular towers, and they deactivated the towers at night, preventing US intelligence operations.

Another dimension of concern is MTN's decades-long association with Hezbollah, a designated terrorist organization and a proxy of Iran. This relationship involved providing equipment that Hezbollah used as detonators and for tracking their adversaries. This history of supporting and enabling terror activity might indicate that other proxies of Iran, such as Hamas were also benefiting from MTN's services.

There is evidence that Hamas' brutal attacks against Israel, were accompanied by cyberattacks conducted by a group linked to Iran. The attacks were aimed at stealing, publishing, and deleting sensitive information such as personal data and

intellectual property from educational institutions and tech companies. These attacks began in January 2023 but were intensified following the October 7th attacks.

NYT reported that Iranian hackers were waging an espionage campaign targeting rivals across the Middle East, including Israel, Saudi Arabia, and Jordan. The cyberattacks are linked to Iran's Ministry of Intelligence. According to Israeli cybersecurity officials, 15 groups of hackers, such as "agonizing serpens" and "LionTail", affiliated directly or as a proxy, with the IRGC and Iranian Ministry of Intelligence, are responsible for the attacks. During this campaign, there were also attempts by groups affiliated with Hamas and Hezbollah to hack CCTV cameras in Israel.

It's time to stop Iran

As shown above, Iran's terror network is broad, and it also serves as a distraction from its efforts to cross the nuclear threshold and reach a nuclear military capability. Following Iran's involvement in Hamas' attacks against Israel and the continuous support of other proxies in the Middle East, the international community must to step up joint efforts to stop both Iran and its accomplices.

The most common measure against Iran is sanctions, mainly in relation to the nuclear program. While sanctions took a toll on Iran's economy, the shadow financial network provided it a lifeline. This year, the US imposed new and broader sanctions on a "shadow banking" network of 39 entities across multiple jurisdictions, including those registered in China, Türkiye, and UAE. These sanctions are targeting Iranian front companies abroad that have generated tens of billions of dollars for the Iranian regime.

One of Iran's ways to bypass sanctions is the use of cryptocurrencies, which Tehran legalized in 2019. Around 4.5% of global bitcoin mining is done in Iran. International compliance regulations, including those issued by the FATF (Financial Action Task Force), have made it more difficult to use cryptocurrencies as a way to evade sanctions but did not entirely stop Iran.

In addition, the US decided to freeze $6 billion that was part of a prisoner swap deal with Iran to free 5 American citizens. Due to Iran's backing of Hamas, the US reached an understanding with Qatar to prevent access of Iran to the funds. The US also imposed new sanctions on Hamas and members of IRGC for arming,

training, and providing financial assistance to the terror organization. The US Department of Treasury emphasizes Iran's role in providing financial, logistical, and operational support to Hamas.

The EU announced that it is considering imposing similar sanctions against Iran over its support of Hamas. Moreover, the big three European countries refused to lift sanctions on Iran after the 18th of October 2023, a date set by the original deal in 2015 and relates to missile capabilities of Iran.

Although there is still some pressure on Iran, the effectiveness of sanctions is debatable. The Iranian leadership is very flexible in its ways to evade sanctions, leaving the Iranians to suffer as a result of the sanctions, especially when these are focusing on financing channels. Yes, the economy plunged but that did not change the behavior and ambitions of the Iranian regime.

The current situation in the Middle East generates an opportunity and momentum to act now against Iran. This should include complementary means to sanctions, such as cyber tools, a direct credible military threat to Iran's strategic infrastructure, and dismantle of its proxies. But also, the targeting of target channels of technology transfer and financial support with direct links to IRGC. In this context, the lawsuit against MTN Group is an important step. The Iranian leadership and its accomplices must know that as long as they engage in terrorism and nuclear armament, the international community will react vigorously.

Published in The National Interest 04.12.2023