Albania Terminated Diplomatic Relations With Iran Over Cyber-Attack

written by Ezba Walayat | September 16, 2022

Introduction

Albania and Iran have had tense relations ever since Albania accepted over 3,000 members of the Iranian opposition group People's Mujahideen Organization, also known as Mujahideen-e-Khalq in Farsi, who had set up camp outside Durres, the country's major port, in 2014. Recently, the tensions have further escalated between the two countries over a cyber-attack as Albania claims that the country has evidence which reflects the direct involvement of Iran behind the cyber-attack. The Albanian Government has experienced a significant cyber-attack on July 15, as per reports hackers destroyed the data, shut down the government service e-portal and exposed information about the Prime Minister and Ministry of Foreign Affairs. In a video statement, Prime Minister of Albania Edi Rama stated that the Government has made the decision to sever diplomatic ties with the Islamic Republic of Iran, to be effective immediately. He continued by saying that the hacking group's objective was the damage of the Republic of Albania's Government's digital infrastructure, as well as the theft of data and electronic communications from networks base on Government level.

FILE – Albanian Prime Minister Edi Rama pauses before speaking as he addresses a media conference at EU headquarters in Brussels, Tuesday, July 19, 2022. Albania cut diplomatic ties with Iran and expelled the country's embassy staff over a major cyberattack nearly two months ago that was allegedly carried out by Tehran on Albanian government websites, Prime Minister Rama said Wednesday, Sept. 7, 2022. (AP Photo/Virginia Mayo, File)

UK And The United States Support To Albania

In contemporary times, NATO member Albania is the first Government to be known to have terminated diplomatic ties with another country in reaction to a cyber-attack and gave the diplomats, security officers, and employees of the embassy in Tirana 24 hours to leave the country. The decision to expel its ambassadors was criticized as being "anti-Iranian", and a statement made in response hinted that "third parties" may have been involved in the charges which points the U.S. indirectly. Albania's action was backed by a number of countries, including the United States and the United Kingdom. However, Albania's decision to sever diplomatic ties with Iran was strongly opposed by Tehran, according to the Iranian Foreign Ministry, Albania's justifications have been rejected while considering them as baseless allegations. The hackers, which had ties to Iran, carried out a cyber-attack using malicious data-wiping software targeting Iranian opposition group, according to Mandiant, a U.S. cyber-security company that first reported the hacking activity. The attack was carried out by one or more threat actors who have acted in support of Iranian objectives, as per Mandiant, which stated it had reached this conclusion with confidence. After weeks of inquiry, the United States claimed it had come to the conclusion that Iran was responsible for conducting a reckless attack. In order to hold Iran responsible for activities that endanger the security of a U.S. ally and create unfavorable precedent for cyberspace, the United States will take

additional measures has said by U.S. National Security Council in a White House statement. This could result in creating more tensions between the U.S. and Iran as the United States firmly denounced the cyber-attack on a NATO ally and vowed to hold Iran responsible for any actions that endangered Albania's security.

Conclusion

The history shows that there have been major cyber incidents occurring for many years which caused threat to high tech, defense and government. Today, a number of actors have access to cyberspace for geopolitical influence or financial advantage as a result of the proliferation and commodification of cyber offensive capabilities. Countries have interfered in elections, halted public services, infiltrated IT infrastructure with malware, and even disrupted adversary security systems during the past few years. The capability of technology and the reach of the internet, along with creative thinking, have altered how nations engage in warfare. It is alarming, if the nation-states use offensive cyber-attacks whether against one another directly or by enlisting the help of cybercriminals, it will leave people vulnerable and complicate the existing complex cyber threat scenario. It is a time when the internet is relied upon for both domestic and international benefits. Many experts predict that over the coming years, cyber warfare will both expand and become more complex. Global cyber security threats have become a serious challenge, and every government needs to take greater action in the area of cyber security and maintain a specialized unit to combat cybercrime by performing their fair share and positive part to prevent, identify, and lessen the impacts of cyber-attacks through cyberspace governance and investing in the appropriate strategies.