Cyber-attacks lead to conventional military strikes

Reference: Memo [190507-1] Date: 07/05/2019 - Version: 1.0
Keywords: conventional strike, retaliation, military, defence, cyber-war
Sources: publicly available information

Key Points

- Israel Defence Forces destroyed the headquarters of the main cyber unit of the Palestinian organisation Hamas by airstrikes.
- The assault is likely to be the first true example of a physical attack being used as a real-time response to digital aggression.
- Affected entities will likely rebuild their lost capabilities and continue to conduct cyber operations against Israeli targets.

Summary

On May 5, a spokesperson for the Israel Defense Forces (IDF) stated that Israeli airstrikes had destroyed the headquarters of the main cyber unit for the Gaza-based Palestinian organisation Hamas. In this statement, the spokesperson said: "We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed." According to Israeli officials, the IDF struck the unit after thwarting an unspecified Hamas cyber operation aimed at "harming the quality of life of Israeli citizens".

On May 3, a member of the Palestinian Islamic Jihad (PIJ) shot two Israeli soldiers near the Gaza-Israel border, prompting an Israeli military response. In the weekend, the escalation of violence left 31 Palestinians and 4 Israelis dead. Final casualty counts continued to climb on May 6.

The Israeli response to the malicious cyber operation was reportedly conducted as a joint effort by the IDF's Unit 8200 of Military Intelligence along with the IDF Teleprocessing Directorate and Israel's internal security service, Shin Bet.

Comments

Amid an intense exchange of fire between both parties, the assault is likely to be the first true example of a physical attack being used as a real-time response to digital aggression.

In 2015, in an action planned over many months, a US airstrike killed Islamic state hacker Junaid Hussain. However, this strike was not a real-time response and Hussain was targeted for not just hacking, but for serving as a key player in broader ISIS recruiting strategies.

NATO has recognised cyberspace as a domain of operations in which it must defend itself as effectively as it does in the air, on land and at sea. This likely means that just as Israel, NATO does not rule out using kinetic means to defend assets in cyberspace.

With the May 2019 attack and the statement to the press, Israel highlighted its willingness to use kinetic military response to Hamas' cyber operations. This tactic will likely become more common in future Israel military operations in Gaza.

A number of cyber-threat actors and cyber-operations have been connected to Hamas or other entities based in Gaza in the past few years by cyber-security firms. The firms assign them code names such as Molerats, Gaza Cybergang, Gaza Hack Team, Gaza Hackers Team or Extreme Jackal. Since about 2012, these entities have participated in hacktivist campaigns such as OpIsrael (defacements, DDoS). They have also exhibited moderate skills for customisation and deployment of malicious tools, malware, and associated infrastructure for targeted intrusions and espionage. It is likely the Gaza cyber entities affected by the Israel strike will rebuild any lost capabilities and continue to conduct cyber operations against Israeli targets.

CERT-EU is tracking these threat actors under its threat actor's knowledge base programme. This means that CERT-EU will continue refining its knowledge of the group's profile, identify its techniques, tactics and procedures (TTP), and collect and share actionable threat data related to this group. If the threat actors become a direct threat to EU institutions, bodies and agencies, CERT-EU will release a threat alert with relevant actionable information. Should you need more information on this group or on our threat actor's programme, please contact CERT-EU.