Operation Protective Edge: The Cyber Defense Perspective

Daniel Cohen and Danielle Levin

Cyber warfare has become an important source of power for nations, and at the same time is a strategic threat to a nation's critical infrastructure, given that communications, media, finance, and many other sectors now rely on the cyberspace domain. Militaries in particular have become heavily reliant on advanced cyberspace technology. On a national level, Israel is in the process of establishing an integrated national cyber defense system, which demands cooperation between the civilian sector (civil service and private) and security and military establishments.

The Israeli defense system against cyber attacks during Operation Protective Edge tested Israel's utilization of government policy in the cyber sphere, and marked a significant improvement in coordination between Israel's cyber defense organizations, including the functioning of Israel's IT security systems and the increasing cooperation between the civilian and defense sectors. This article examines the cyber attacks during Operation Protective Edge, analyzing three major factors: the volume of attacks, the actors behind the attacks, and Israel's advances in cyber security.

Volume of Cyber Attacks against Israel

A serious increase in the number of cyber attacks accompanied the entry of IDF ground forces into the Gaza Strip during Operation Protective Edge. Some of these attacks can be attributed to organized cyber rallies of amateur hacking groups, while other cyber attacks verged on a more sophisticated level that focused on Israeli communication networks. Once the ground operation concluded, the number of cyber attacks declined significantly.[1]

One of the major cyber attacks during the operation focused on communication and internet suppliers aiming to overload the system and cause Israeli networks to collapse.[2] More generally, the attacks included distributed denial of service (DDoS) and Domain Name Service (DNS), the collapse of over 1,000 non-crucial Israeli websites, website defacement, exposure of databases, and leaked personal information of Israelis such as login credentials.[3] Each exploit generated additional opportunities for Hamas to gather more data, as new potential targets were identified. In addition, tailored methods and means of approaching these targets were developed, such as when Hamas sent mass text messages to Israelis claiming to be either from the Israeli Security Agency (ISA), *Haaretz*, or Hamas.

Additional attacks included interference with a private television satellite, which allowed a pro-Hamas propaganda message to appear momentarily on Channels 2 and 10 (Hamas launched a similar attack against commercial channels during Operation Pillar of Defense).[4] The IDF Spokesperson's blog and Twitter account faced a major cyber attack conducted by the Syrian Electronic Army (SEA), with messages posted in English and Arabic.[5] In addition, large hacking groups coordinated multiple cyber protests against Israel, referred to as "OpIsrael." These operations brought major cyber groups to work together throughout the operation for the Palestinian plight.[6]

The Actors behind the Attacks

Throughout the operation, the IDF cooperated with ISA to foil planned attacks by Iran on al-Quds Day, an annual event organized by Iranian leaders against Israel. The attack involved hackers from all over the world who attempted to disable Israeli websites.[7] Over the last few years, major terrorist groups such as Hamas and Hizbollah, with assistance from Iran, have demonstrated an increasing interest in the field of cyber terror. State sponsored cyber terrorism groups like the Iranian Cyber Army and SEA executed cyber attacks during Operation Protective Edge, and overall, the IDF maintained Iran had a major role in the increase of cyber attacks targeting civilian facilities during the operation.[8]

Another group targeting Israel, but not openly identifiable from the Muslim and Arab world, was the hacking collective Anonymous, which in regard to attacks against Israel is divided into three units: Arab, Muslim, and the remaining collective. Anonymous, which previously organized cyber operations against Israel, can consist of elite hackers, yet Operation

Protective Edge was distinctive in that this caliber of hackers decided not to participate.[9] This potentially provides an explanation for the distinction between Operations Pillar of Defense and Protective Edge regarding the identity of attackers. In Operation Pillar of Defense, the Israeli government faced over 100 million cyber attacks in eight days, with IP addresses tracing back to sites all around the world, predominately from Europe and the United States.[10] In comparison, during Operation Protective Edge, a cyber security company report estimated that 70 percent of cyber attacks could be traced back to Arab and Muslim countries.[11]

Israel's Advances in Cyber Security

Israel took a proactive cyber approach with a pre-planned defense strategy of advanced operational capabilities that provided a high proficiency of security defense.[12] Both the IDF and the ISA were able to foil any attempts to damage Israeli government networks and critical infrastructure. The ISA confirmed it was able to secure all Israeli government networks and systems against cyber attacks. One of the defense methods was to block foreign IPs for two hours at the start of Operation Protective Edge. ISA, through its cyber division, acted in coordination with private contractors, the Israeli Ministry of Communications, and the media in taking preemptive measures against the attacks.[13]

The IDF worked with an integrated communications network of Military Intelligence and cyber companies related to the Ministry of Defense, which assisted in recognizing and removing all cyber threats from attackers. The head of the IDF cyber defense unit claimed that infiltration of IDF networks had also been attempted, and asserted that Israel's high technological capabilities were elevated in order to ensure breaches did not occur.[14]

Conclusion

Cyber cells of terrorist organizations have so far been unable to execute strategic cyber attacks against Israel, which requires high levels of intelligence and technological capabilities. Terrorist organizations are presumably improving and developing advanced cyber capabilities that could pose a future threat to the cyber sphere. This threat is interconnected between terror organizations and state sponsored terrorism, which includes deception via hacktivist groups. Israel cyber security defense perspective should recognize this link as a national security threat.

The implementation of cyber regulations and preventive action aims to make cyber protection a built-in necessity to protect the Israeli state, including the civilian sector (private and public). It is imperative to acknowledge these sectors as part of the national security infrastructure.[15] There was a significant improvement in coordination of Israel's cyber defense organizations during Operation Protective Edge, including the functioning of Israel's security IT systems and the increasing cooperation between the civilian and the defense sector. This experience underscores the immediate need to formulate a protocol for defense of civilian cyberspace.[16]

Notes

1 IDF Blog, "The Attack against Israel You Haven't Heard About," August 22, 2014, http://www.idfblog.com/blog/2014/08/22/attack-israel-havent-heard/.
2 Jonathan Lis and Oded Yaron, "Amid Cyber Attacks on Israel, Security Agency Wins a Battle Fighting Back," *Haaretz*, July 28, 2014, http://www.haaretz.com/news/diplomacy-defense/.premium-1.607479.
3 See Anonymous sub-group, AnonGhost Pastebin: http://pastebin.com/Lq6geBuJ.
4 "Watch: Hamas Hacks into Channel 10 Broadcast," *Jerusalem* Post, July 14, 2014, http://www.jpost.com/Operation-Protective-Edge/WATCH-Hamas-hacks-into-Channel-10-broadcast-362767.
5 SEA tweets on the IDF Twitter included "Long Live Palestine," and "#WARNING: Possible nuclear leak in the region after 2 rockets hit Dimona nuclear facility."
6 Daniel Cohen and Danielle Levin, "Cyber Infiltration during Operation Protective Edge," *Forbes*, August 12, 2014, http://www.forbes.com/sites/realspin/2014/08/12/cyber-infiltration-during-operation-protective-edge/.
7 IDF Blog, "The Attack against Israel You Haven't Heard About."
8 Gabi Siboni and Sami Kronenfeld, "The Iranian Cyber Offensive during Operation Protective Edge," *INSS Insight* No. 598, August 26, 2014, http://www.inss.org.il/index.aspx?id=4538&articleid=7583.
9 Cohen and Levin, "Cyber Infiltration during Operation Protective Edge."
10 David Shamah, "Steinitz: Israel Beat Back 43,999,999 and a Half Cyber Attacks," *Times of Israel*, November 12, 2012, http://www.timesofisrael.com/steinitz-israel-beat-back-43999999-and-a-half-cyber-attacks/.
11 David Shamah, "Qatari Tech Helps Hamas in Tunnels, Rockets: Expert," *Times of Israel*, July 31, 2014, http://www.timesofisrael.com/qatari-tech-helps-hamas-in-tunnels-rockets-expert/.
12 Shamah, "Steinitz: Israel Beat Back 43,999,999 and a Half Cyber Attacks."
13 Lilach Shoval and Eli Leon, "Iran Waged Cyber Warfare against Israel during Protective Edge," *Israel Hayom*, August 18, 2014, http://www.israelhayom.com/site/newsletter_article.php?id=19515.
14 Gili Cohen, "Israeli Officer: Iran Involved in Cyber Attacks during Gaza War," *Haaretz*, August 18, 2014, http://www.haaretz.com/news/diplomacy-defense/.premium-1.611013.

15 Gabi Siboni, Daniel Cohen, and Aviv Rotbart, "The Threat of Terrorist Organizations in Cyberspace," *Military and Strategic Affairs* 5, no. 3 (2013): 3-29.
16 See Gabi Siboni, "A National Response to Civil Defense in Cyberspace," Policy paper, INSS, August 2013.