What ‘Anonymous’ really wanted

By YOAV COHEN

How many Palestinians feel more liberated thanks to #OpIsrael, the targeted cyber-attack launched by the “Anonymous” hacker collective this week? Probably none. In fact, it is hard to believe any Palestinian solidarity ever existed. The sad truth is that this “digital flotilla” had nothing to do ending Palestinians woes. Anonymous, like the IHH, decided to jump on the “bash Israel” bandwagon to raise awareness and money for themselves.

This was the first time an organized group launched a coordinated attack against a collection of public and private Israeli websites. But, like the infamous Turkish flotilla to Gaza in 2010, #OpIsrael had all the signs of a public slur campaign with ulterior motives. Anonymous used the right rhetoric and timing to get the media’s attention and force Israeli government officials, companies and individuals to open the virtual situation rooms. Twitter fans began following, the news outlets bit, the headlines ran and the stage was set, as in the case of the flotilla, for the showdown.

Did Anonymous achieve any of their declared goals? A large number of government and private websites were attacked. Approximately 60 million attacks were reportedly launched, of which a minuscule number were successful. Certain sites were overloaded with data requests until they crashed, known as DDoS (Distributed Denial of Service) attacks. Other smaller and less protected sites were compromised, their homepages replaced with dark graphics, empathic Palestinian photos, anti-Israel messages and dramatic music. Ask the Anonymous hackers (if you could) and they would claim victory.

Yet, these types of attacks are nothing out of the ordinary. Israeli websites are always under threat from hackers seeking to leak sensitive information or to bring down “ill” domains and servers. The significance in the #OpIsrael campaign lies in the increased scale and concentrated timeframe, not in the capabilities of the hackers or their achievements.

As soon as Anonymous tweeted about hacked “goliath” websites, these were back online. Smaller sites took a little longer to revert to their original state, but this was nothing more than a nuisance, as in the case of the “Women of the Wall” website. (Gaza-liberating hackers apparently do not favor gender equality.) Other private websites hacked seemed to hardly be protected or active. If anything, Anonymous brought extra traffic to sites struggling to attract visitors. In the end, no electricity plants crashed. No one lined up outside their bank to withdraw money in panic. Israelis happily continued to snap Instagram pictures, share them on Facebook and hit the “like” button.

Did #OpIsrael help the Palestinians in any way? No, and it was never meant to. Anonymous set out to raise awareness about a conflict that people around the world are already aware of if they ever watched TV or visited a news website. They did not expose devilish secret protocols as Wikileaks attempted to do, nor did they cause any lasting damage, as Stuxnet did. Their aim was simple: put Anonymous back in the headlines.

Branding a campaign with anti-Israel slurs and using footage from previous military operations in Gaza and the West Bank is extremely simple, yet effective. Conveniently, the campaign advertised Anonymous’s own fundraising efforts, by “tweeting between the lines” about Anonymous’s activities, associates and sympathizers. AnonNews is one example. Funded by donations, the anti-corporation news website managed to attract hundreds of donations, amounting to thousands of dollars, during #OpIsrael. Anonymous’s plan actually backfired on the Palestinians and any future virtual Inifada. Instead of wreaking havoc, hackers provided a pre-planned scenario and training operation for Israel’s counter-terrorism units, high-tech system administrators, ISPs and watchful individuals. They all took the threat seriously, dealt with it successfully and went home to eat dinner.

Despite the minimal damage caused this week, it is imperative to remember the responsibility of the sensible and literate computer user, and to take precautions to limit virtual or real harm. ISPs, email providers and system administrators encourage strong passwords for a reason. Anti-virus software is a basic necessity. While it is tempting to believe that you have been arbitrarily selected to receive a prize from a website, or that a friend visiting Bhutan needs your financial assistance, this is probably not the case.

Free emotions are nothing more than Trojan horses, malware and other malicious software. Even on trusted social media websites, the information uploaded is potentially public; no matter what privacy settings have been set. The real rule of thumb is to simply think before you click.

With more personal information available than ever before in history, cyberterrorism and cyberwarfare are a reality not to be taken lightly. Stuxnet, Stuxnet and other high-end computer viruses proved capable of causing virtual and physical damage to extremely advanced systems and networks, even destroying them. While Anonymous hackers seem far from these capabilities, they did demonstrate a scenario that will likely repeat itself in the future. The more hacktivists have time and systems at their disposal, the more we will see such attacks, probably without warnings.

Had Anonymous members really wanted to help Palestinians, they might have invested their resources in computer centers in Gaza and their talents and time fostering digital literacy to children who need it most. #OpIsrael was another anti-Israel campaign meant not to improve the Palestinians’ reality, but instead serve the private needs and wants of the initiating organization. In the meantime, Syrians still die and Egyptians still protest – but these are less attractive posters to donors and news editors.

The author is currently the manager of the Argov Fellows Program at IDC Herzliya and the director of operations for http://www.friendsoldsolider.com, an independent dialogue website.