Forbes

Opinion

8/12/2014

Cyber Infiltration During Operation Protective Edge

Daniel Cohen & Danielle Levin

At the commencement of Operation Protective Edge, the latest Israeli military operation in the Hamas-governed Gaza Strip, hackers began attacking Israeli government sites and media outlets through denial of service (DDoS) and Domain Network System (DNS) attacks, and the personal data of Israeli citizens were exposed. These recent attacks are connected to cyber groups with links to state sponsorship terrorism, with some affiliation to the Anonymous theoretical concept. When regarding the Anonymous collective association with attacks aimed at Israel, the Anonymous collective can be divided into three cells: Arab, Muslim, and the remaining collective. In terms of capabilities and adroitness, the first two groups usually merge, while the third group is more proficient and sophisticated. Operation Protective Edge marked a shift in perception regarding Anonymous' stance and actions, causing the public to question whether Anonymous and other hacktivist groups are being infiltrated and deceived by Hamas and other pro-terrorist organization affiliates, or are these groups merely sympathizers.

One of the initial cyber attacks against Israel breached over 1,000 Israeli websites, though majority of these websites were deemed non-crucial (Anonymous claimed otherwise). In addition, Israeli Internet providers were redirected and foreign IPs were blocked for several hours. Also, the IP and email addresses of Israeli ministry workers were exposed. The attack had little to no significant impact as most of the websites recovered within hours and the information had been published in previous attacks. The Israeli Security Agency announced they contained all attacks against government and military networks. As one of the main goals of hacktivism is bringing attention to a social or political cause, more cyber protests were arranged. However, each organized cyber operation became increasingly repetitive causing little media circulation. One of the most prominent examples was on 25/07, when Anonymous implored elite hackers to join but no major attack was reported and Israeli networks ran as usual.

So far, there has been no demonstration of high technological and intelligence capabilities in cyber attacks against Israeli networks by terror organizations independent cyber units. To operate a successful cyber attack requires determination of targets, timing of the attack and cyber tools. Terror organizations have yet to cross the independent operational and technological thresholds to conduct cyber warfare independently against Israel and other countries. Terror organizations, like Hamas and Palestinian Jihadic Islam, possess very limited technological capabilities and resources. Yet, there are cyber terrorist groups with affiliation to states, such as the Syrian Electronic Army and Iranian Cyber Army that are capable of producing more advanced cyber operations.

Meanwhile, pro-Gaza rallies have increased the amounts of anti-Semitic incidents, especially in Europe, to the extent that a prominent Anonymous Twitter handle commented on the perturbing situation. Though Anonymous did not dismiss their protests, it became incontestable that major cyber attacks were largely reduced. The anti-Semitic conclusion to many of the pro-Gaza rallies made hacktvisits within the community question Anonymous' pro-Arab initiative; many voiced that the Anonymous pursuit for justice took a pro-Palestinian slant, and its involvement in the Israeli-Palestinian conflict has lead to accusations of anti-Semitism.

When members of the Anonymous collective are faced with the assumption that terrorist groups may have infiltrated certain Anonymous divisions for their own agenda, many hackers responded by stating anyone can join Anonymous; however, those taking advantage of the Anonymous collective to gain publicity will have trouble sustaining long-term cyber attacks. Additionally, some members believed the notion of cyber terrorists in Anonymous is an idle threat rather than a real concern. When confronted with the rising anti-Semitic wave, many members deflected by focusing on Israel or shifting to the identity of the "true" enemy.

The link between terror organizations, state sponsor terrorism, and deceived hacktivist groups should be recognized and acknowledged as a national threat. The terror organizations infiltrating hacktivist groups such as Anonymous should be met by preemptive government measures. Preventive action includes targeting the operator's resources from websites to finances. The parties involved must be exposed, charged and convicted for terror acts.

Other steps include preventative exploratory actions. First, to increase awareness of the possibility that operators may be held responsible for facilitating hacking or cyber attacks. The second is identifying the operators of the cyber attacks. As noted, in many cases the cyber attackers have been deceived and are completely unaware they are being operated by state sponsored terrorist organizations. It is, therefore, possible that these actions can reduce the scope of the phenomenon.

The major differences between cyber attacks conducted during Operation Pillar of Defense and of Operation Protective Edge lies in the amount of cyber attacks, Israeli advancement in cyber security, and the actors involved. In comparison to Operation Pillar of Defense, were the Israeli government faced over 100 million cyber attacks in eight days and IP addresses traced back to Europe and the United States, during Operation Protective Edge, 70 percent of cyber attacks were traced back to Qatar, Hamas' main benefactor. The major public cyber attacks were not conducted by sophisticated Anonymous hackers but rather executed with the capabilities of cyber terrorists.

The cyber case study during Operation Protective Edge illustrates the relevance of applied explanation to hacktivists communities all over the Internet, as part of national defense perception. This case study is also relevant to participants active in the non-virtual sphere, and represents the necessity of explanation in social media networks and in physical demonstrations, and can be a tool against deception.

Daniel Cohen *is a Researcher at the* ***Institute for National Security Studies (INSS)*** *at Tel Aviv University*. ***Danielle Levin*** *is Research Assistant in the Cyber Security Program at INSS*.

http://www.forbes.com/sites/realspin/2014/08/12/cyber-infiltration-during-operation-protective-edge/