INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

INSS Insight No. 521, February 26, 2014

SEA: How Real is the Threat?

Daniel Cohen and Danielle Levin

The threat of cyber terrorism has created the image of a terrorist in a remote, isolated location inflicting major damage by penetrating security or economic systems via cyberspace, and this image has been made especially popular through the activity of the Syrian Electronic Army (SEA). With hackers targeting popular websites, SEA has brought the image to the fore of global threat perceptions. But when examining the cyber terrorism threat, it is necessary to scrutinize the actual capabilities of terrorist organizations like SEA in the cyber realm, to analyze whether there is indeed a substantive, powerful threat inherent in their cyber attacks.

The existing documented information on SEA depicts it as comprising a group of young, political hacktivists supporting Syrian President Bashar al-Assad in Syria's civil war by conducting malicious cyber operations against Syrian opposition and Western websites. The SEA membership is unknown, and the group identifies itself as decentralized. Besides SEA's pro-Assad messages, many believe the Syrian government is connected to the group. SEA was originally registered with the Syrian Computer Society (SCS), which caused further speculation that SEA's roots lay in SCS, as in 1990 Assad was president of SCS. Assad referred to SEA as a "virtual army in cyberspace," and SEA held a domain hosted by the Syrian government before being indefinitely suspended in June 2013, when key Syrian government officials were arrested. Speculation on government collaboration persists, yet the only substantial evidence of government involvement is SEA's ability to operate within the restrictive regime and, as SEA expert Helmi Noman stated, connections do not seem to go beyond "tacit support."

SEA focuses primarily on gateway attacks, the most basic level cyber attack on an organization's gateway (i.e., internet webpages), which by nature is exposed to the public. SEA breaches these sites on a regular basis, and phishing (stealing) passwords is considered its biggest success. The cyber group has broken into more than 120 websites, including high media organizations such as the *Financial Times*, *The Telegraph*,

Daniel Cohen is the Coordinator of the Cyber Warfare Program and the Military and Strategic Affairs Program at INSS. Danielle Levin is an intern in the Cyber Warfare Program at INSS.

Washington Post, and *al-Arabiya*, and third party communication sites as Viber and Tango. One of the most significant and effective attacks occurred in April 2013, when SEA broke into the Associated Press's Twitter account, implanting a tweet asserting the White House had been bombed and President Obama was injured. The immediate consequence was a sharp drop in the US financial markets of more than $100 billion and a steep drop in the Dow Jones Industrial Average for several minutes. SEA has hacked Twitter handles of inconsequential entertainment websites that do not advance their cause, such as *E! Online* and *The Onion*, suggesting that SEA relishes the attention gained by exposing its platform to the unacquainted and uninvolved websites.

SEA first emerged in April 2011 by defacing and spamming Facebook groups, with posts of the SEA logo and pro-Assad messages such as, "Sorry, we do not want to destroy your official website, but the British Government actions and attitudes against Syria and its interfering in the Syrian internal affairs forced us to step forward and break through your website." On January 19, 2014, SEA hacked and defaced 16 Saudi Arabian government websites, posting messages accusing Saudi Arabia of terrorism, and forcing all 16 websites offline. Microsoft has been a repeated target of SEA, which hacked email accounts through phishing for the second time in the span of a few months and obtained and published personal data of Microsoft employees and users. However, the most alarming aspect was SEA's declaration once it suspended its attack, tweeting shortly afterwards: "we didn't finish our attacks on @Microsoft yet, stay tuned for more." Even more recently, SEA hacked PayPal UK and *Forbes* and sprinkled their websites with messages in support of the Syrian regime. Regarding the PayPal attack, SEA stated that no personal user data had been breached, and the purpose of the attack was to respond to PayPal's refusal to allow Syrians to use their operating system.

The publicity of each SEA attack causes a flurry of media attention, emphasizing the urgency of cyber security in the media community. Analysts claim there is little to stop Syria in this regard, considered the first Arab country to have a public Internet army. Yet while SEA cyber attacks cause paralysis and disruption, they rarely cause substantial, irreversible, or lasting damage, and hacks remain more embarrassing than destructive.

To date SEA has limited its activity to public forum attacks, which focus on defacing and hacking public websites and social media pages. This circumscribed scope is likely due to the fact that terrorist organizations are hindered by curtailed access to technology. The internet enables cyber weaponry trade, making it easy for SEA to gain the necessary tools for gateway attacks. Indeed, hackers and traders exploit these advantages and offer cyber tools and cyberspace attack services to anyone seeking them. Nevertheless, more sophisticated cyber attacks are unrealistic, as acquisition of the means to undertake them is limited to countries with advanced technological proficiency or state sponsored terrorist organizations.

SEA has not developed to the point where it can cause irreversible damage. It lacks the requited high quality intelligence for cyber operations, along with the necessary large scale personnel, monetary investment, and time to detect vulnerabilities. SEA has succeeded in conducting low scale attacks, which at the right time and place can cause damage through side effects, as in the hacking of AP’s Twitter account. However, the image of the isolated terrorist responsible for a catastrophe is not borne out, as cyber terrorism such as waged thus far by SEA is incapable of causing long term sustainable damage.