INSS Insight No. 464, September 10, 2013

Backdoor Plots: The Darknet as a Field for Terrorism

Yotam Rosner, Aviad Mendelbaum, Sean London, and Yoram Schweitzer

On Friday, August 2, 2013, the US State Department published a travel warning, and in an unprecedented step, closed over twenty embassies. As expected, following the American warning other Western countries such as Great Britain, France, and Germany ordered the closure of various embassies. Several days after, the alert was reported as a response to the monitoring of a conference call among a team of terrorist leaders, including al-Qaeda's Ayman al-Zawahiri and the heads of its affiliate organizations. It was gradually reported by anonymous intelligence sources that the information was found in the possession of an al-Qaeda courier who had recordings of the call. Minutes of the call were transmitted via the internet, and there was also a seven-hour recording of the entire call. By tracking the courier, the United States succeeded in discovering the call, which apparently took place in a part of the internet sometimes called deepnet, blacknet, or darknet.

The global battle against terror has done serious damage to al-Qaeda's physical infrastructures, and thus to limit its exposure, al-Qaeda has stepped up its activity in cyberspace. Activists have learned to exploit internet technologies by using known networks to distribute material for recruitment, training, and coordination of terrorist operations. In the late 1990s, there were several dozen websites connected to terrorist organizations; in 2005, more than 4,000 such sites were documented.

The internet has a visible side and a hidden side. The visible side includes sites that can be found through an ordinary search, while the hidden side, called the darknet, includes sites or networks that cannot be accessed by regular means. These sites serve as a platform for internet users for whom anonymity is essential, since darknet sites not only provide protection from unauthorized users but also usually include encryption to prevent monitoring.

Yotam Rosner and Aviad Mendelbaum are interns in the Terrorism and Low Intensity Conflict Program at INSS, headed by Yoram Schweitzer. Sean London, formerly a research assistant in the Terrorism and Low Intensity Conflict Program at INSS, is a media adviser in New York.

The obscure regions of the darknet have allowed al-Qaeda to adapt itself to the restrictions imposed by the international system and operate as a virtual terror network. A study published in 2011 reported that the darknet has more than 50,000 sites and 300 forums for terrorist organizations. Moreover, for about a decade, open sources have reported that while global jihadi activists exploit darknet for the purposes noted above, the network is mainly a platform for direct communication among leaders and organization activists. Therefore, that the darknet was used for a conversation among senior al-Qaeda officials is not surprising, and in fact, al-Zawahiri, CEO of al-Qaeda Terrorism Inc., exploits the technology at his disposal in order to communicate regularly with his senior "managers".

Many of those on darknet use TOR (The Onion Router), a free download that enables the user to remain anonymous. As noted on its homepage, TOR prevents monitoring of websites that users visit, makes it impossible for websites to learn the user's physical location, and enables users to circumvent internet censorship. Furthermore, TOR prevents identification of website managers who do not wish to be identified.

Last June, Ofir David of cyber defense company CyberHat reported a security breach in Mozilla Firefox versions 17 and 22 that resulted in the exposure of users' identity; Mozilla subsequently confirmed that there had in fact been a breach. In August it became apparent that many other sites in the darknet had been hacked or completely blocked. Several days later, Eric Eoin Marques, who had been exposed as "the largest facilitator of child porn on the planet," was arrested. Apparently, this was a sting operation by the FBI intended to prevent the distribution of child pornography online. According to David, "Whoever is running this exploit can match any TOR user to his true internet address, and therefore track down the TOR user." This breach clearly caused significant harm to TOR's effectiveness as a provider of anonymity.

The proximity of Marques's arrest to that of the arrest of the al-Qaeda courier and the centrality of the darknet in both cases raises the possibility that the two were connected. According to this hypothesis, US authorities exploited the breach of TOR in order to monitor al-Qaeda officials and the child pornographers, and their exposure by David forced them to act against their targets prematurely because they feared the targets would change their methods of communication following exposure of the breach. This hypothesis also provides a possible explanation for the aggressive UAV attacks initiated by the United States in Yemen around the time of the courier's arrest, which led to the deaths of thirty-four al-Qaeda activists. Nevertheless, researchers who claimed that there was a connection between the State Department's warning and the extensive breach of TOR have in many cases backed down from their claims, because the information that led to the exposure of the pornography network did not match the source of the information that could have led to the monitoring of the conference call, even though there are still those who claim that there is a low probability of accidental contiguity between the two

Reports on the operation increased public awareness of the existence of the darknet and led to a public discussion on the right to privacy vs. homeland security. Among proponents of online privacy, the darknet looks romantic, a safe arena for underground political discussion. In a world that mourns the death of privacy at the hands of the NSA and the like, the darknet allowed opposition figures, journalists, and separatists to publish information while evading censorship and monitoring. It thus made it possible to diffuse facts and ideas that are not compatible with the interests of authoritarian regimes. However, the recent events have made the public aware that the darknet is not only a platform for political discussions, but also an infrastructure for proliferation of weapons and terrorism, along with drugs and child pornography. Furthermore, given the increasing use of the darknet by jihadis and their ilk, it can now be described as a clear and present danger to the security of citizens around the world. Thus, there is a pressing need to create tools that will prevent terrorist organizations (and criminal elements) from harnessing the darknet for their needs.

In recent years, impressive methods have been developed in the West for monitoring content on the visible web, but there is almost no similar arsenal for the darknet. In order to ensure that the necessary tools are developed for monitoring the internet, it is essential to bring up the evidence indicating that the darknet has been turned into a major infrastructure for global terror. Israeli researchers are at the forefront of study of the internet, and therefore, Israel would do well to harness a significant portion of its talents to confront the challenge of darknet. Beyond the enormous contribution to national and global security, such an initiative could open new horizons for Israeli ventures.

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