Chinese Army Prepares for Conflict with United States

Report: Health Alert Issued in Afghanistan Over Waste Disposal

Fact-Checking 'Gasland Part II'

Anonymous Jihad

After NSA leaks Jihadists flock to federally funded Tor network to hide activities

AP

BY: Lachlan Markay

July 1, 2013 11:30 am

Jihadists are seeking out more secure methods of online communications, including an avenue created by the U.S. government and financed by American taxpayers, in the wake of revelations about the U.S. monitoring of online messages.

The Tor network has become a go-to means for jihadists and criminals to communicate, raise money, and buy and sell illicit goods and services without fear of being identified or traced by intelligence or law enforcement officials.

The network uses technology called “onion routing” (Tor is an acronym for The Onion Router), which refers to layers of encryption that prevent governments or other users from obtaining information about users or websites hosted on the network.

Tor uses volunteers’ computers to route traffic through thousands of “nodes” worldwide, obscuring users’ locations and the sources of data hosted on the network. The technology makes it nearly impossible to trace or identify the network’s roughly 500,000 daily users.

The U.S. Naval Research Laboratory created Tor in the 1990s. The network was used as a means to circumvent regimes that censor or block their citizens’ online communications. It is a useful tool for whistleblowers and dissidents who risk retribution by repressive governments.

Tor continues to receive about 80 percent of its funding from federal agencies, including the State Department, the National Science Foundation, and the Broadcasting Board of Governors. None of those agencies returned requests for comment.

The federally funded network is also a hotbed of illegal activity. Through the use of the virtual currency Bitcoin, which also protects user anonymity, criminals have used Tor to anonymously buy and sell drugs, weapons, and child pornography. It has even been used to facilitate contract killings.

Tor “provide[s] a valuable service to many Internet users, particularly those living under authoritarian regimes where accessing certain websites may not be possible or may be tracked in order to identify dissidents,” Robert Knake, international affairs fellow at the Council on Foreign Relations, told the House Science and Technology Subcommittee on Technology and Innovation in 2010.

“Yet these same systems can be used for criminal purposes,” Knake noted. “Standards are necessary for

regulating these services, and they must be promoted internationally."

In the wake of former National Security Agency contractor Edward Snowden's leaks concerning the agency's online surveillance, Tor staff boasted that the network is "a key building block to build systems where it is no longer possible to go to a single party and obtain the full metadata, communications frequency, or contents."

The network cannot fully protect information from being gathered by intelligence agencies, Tor performance developer Mike Perry wrote, but it can help shield information "against some forms of metadata analysis."

Apparently recognizing that fact, web-savvy jihadists stepped up their use of the technology.

Such groups' presence on Tor was reported as early as 2007. By 2009, the Technical Research and Studies Center, a jihadist group that focuses on the use of technology, offered a guide on setting up a Tor browser and improving network performance.

The *Washington Free Beacon*'s Bill Gertz reported in June that terrorist groups and their online supporters have stepped up their use of the network since Snowden leaked information about the NSA's expansive Internet monitoring activities.

Research from other organizations confirmed that reporting.

"After the leak of information regarding PRISM, jihadists alerted fellow supporters about it and advised to continue using encryption programs and other means of security such as Tor to hide their IP address while accessing jihadi forums such as al-Fida', Shumukh al-Islam, and Ansar al-Mujahideen," according to the SITE Intelligence Group, which monitors jihadist activity online.

The network not only protects the identities of users who visit a website but also allows sites to be anonymously hosted on the Tor network itself. Jihadist groups have used that capability to raise money for their cause and offer instructions on building conventional weapons and weapons of mass destruction.

"Fund the Islamic struggle without leaving a trace," one

site hosted on the Tor network pleads. The site—which is accessible through a standard PC web browser—allows visitors to anonymously donate to a jihadist group that says it has members based in the United States and South America.

“We are currently working with recent reverts to Islam and generally training brothers to struggle to establish a new Islamic front both in the U.S. and around the world,” the site says.

It provides a unique Bitcoin key that visitors can use to anonymously donate to the group. Publicly accessible information shows that that Bitcoin account has been a party to four transactions, all in September of 2012.

“We have found that asking for money indicated for these activities attracts far too much surveillance and have decided that we would begin to gather resources through the Internet,” the site adds. Through Tor and Bitcoin, the site can do so anonymously.

Directed to that page, Andrew Lewman, executive director of the Tor Project, denied that it was evidence that terrorist groups use the network.

“Some teenager creates a site, which is just one page of brochureware, and now they’re a terrorist. Ok then,” he said in an email to the *Free Beacon*.

“Maybe it’s run by terrorists who are hunting down IP addresses of press people,” Lewman suggested, noting that accessing the site through a standard web browser does not protect visitors’ identities. “Maybe it’s run by the mob. Maybe law enforcement,” he added.

Lewman insisted that there is “no hard evidence that terrorists use Tor.”

Another jihadist site hosted on the Tor network, this one only accessible through a Tor browser, contains numerous forum posts describing in detail how to construct explosives and chemical weapons.

The site is not accessible without an account, but a publicly available directory of files uploaded to the forum shows that one user uploaded a map of the subway system in the Spanish capital of Madrid to the site at some point in June.

Other Tor Project officials have acknowledged that it can empower nefarious groups and individuals.

“In a free society, there is a balance between freedom for everybody and freedom for the people that you may not like,” Karen Reilly, the Tor Project’s development director, told Reason TV in a recent interview.

“We’re not a democracy-promotion tool,” Reilly said. “We’re not for any particular group of people. We exist to give ordinary people control over their information.”

Law enforcement officials have stated in internal communications that they have no way of obtaining the identities of individuals who use the network to traffic in illegal goods and services.

“Because everyone (all Internet traffic) connected to the Tor network is anonymous, there is not currently a way to trace the origin of the website,” a FBI official said of one investigation into the sale of child pornography on the Tor-based marketplace Silk Road.

“As such, no other investigative leads exist,” the official added. The comments were revealed in documents obtained by the website Muck Rock through a Freedom of Information Act request.

Attempts to break up criminal enterprises that use Tor have ensnared innocent users who simply host Tor nodes through which illegal traffic has, unbeknownst to them, been routed. Those challenges underscore the difficulty of identifying the actual criminal parties who use the technology.

Lewman is adamant that Tor remains content-neutral, lest it practice the type of censorship that it was designed to combat.

“If we even could see the content traversing the circuits, we’d end up re-creating the Internet experience in North Korea; because everyone will demand we censor something different,” Lewman said.

“Terrorists use email, cell phones, web browsers, web forums, Twitter, instant messaging, Skype, Facebook, and all the same technologies you use daily,” he noted. “The moral compass of good or evil is in the human using the technology, not the technology itself.”

This entry was posted in National Security and tagged Islamic Jihad, Tor, Tor Project. Bookmark the permalink.

Lachlan Markay

Email | Full Bio | RSS

Lachlan Markay is a staff writer for the Washington Free Beacon. His email address is markay@freebeacon.com.

MORE FROM LACHLAN MARKAY:

Fact-Checking 'Gasland Part II'
Keystone Pipeline Could Get Boost Following Canadian Train Accident
Gasland Director Presents Anti-Fracking Hoax as Evidence in New Film
Critics: Green Group Abuses EPA Public Petition Process
New Yorker Writer Blames New Yorker Copy Editor for Phony Quote