RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 275 – 7 November 2016

Deep Web: The "Dark" Side of IS

By Shahzeb Ali Rathore

Synopsis

The so-called Islamic State (IS) is the most innovative terrorist group the world has seen. In the backdrop of its loss on the ground, IS is expanding its cyber capabilities to conduct more cyber-attacks and hacking. This and its migration into the 'darknet' will make IS more dangerous than before.

Commentary

TERRORIST AND non-state actors have used different modes and mediums to spread their message and communicate with their comrades. The dawn of the Internet has also provided such groups with unparalleled opportunities to establish communications and operational links that were not possible before. Starting from websites, terrorist groups moved to more interactive mediums like chatrooms and forums. It was social media platforms, such as Facebook and Twitter that truly revolutionised how militants, terrorists and non-state actors communicated with each other, recruited sympathisers and supporters and disseminated their propaganda.

The self-proclaimed Islamic State (IS) perfected the use of social media, which became the preferred source for the so-called 'jihadists' or 'soldiers of the Caliphate'. In response, tech companies have been compelled to take down Facebook and Twitter accounts affiliated with IS. The unintended cost of this policy is that supporters, sympathisers and members of jihadist groups have moved into the deep web and the darknet.

What is Deep Web and Darknet?

The deep web and darknet are terms that are interchangeably used but they are two

different things. The deep web includes all those web pages that a search engine such as Google cannot find. This includes web pages that are password-protected and includes all webmail, private Facebook accounts, user databases and pages behind paywalls. Websites that are not indexed by Google are also considered as part of the deep web. The surface web is all that Google has indexed and a user can access it using any search engine. It is said that the surface web is only the 'tip of the iceberg' and the deep web comprises more than 90% of the total Internet, which is almost 500 times of what Google can see.

The darknet is a part of the deep web but there is an important distinction. We access the deep web every day when retrieving our emails, checking bank statements online or logging into Facebook account. However, we cannot enter the dark net through a regular browser. The darknet is accessed using 'dot onion' software and not a 'dot com' one. As such, dot com browsers such as the Google Chrome and Firefox cannot access 'onion' websites. A different browser, the Tor browser, is used for this purpose.

Tor is an onion browser that sends the user through an unusual route to access a web page. For instance, if a user wishes to access a website using Tor, the browser will wrap the request through numerous layers, which will keep bouncing off different domains in different countries. The layers of the onion (hence the name) ensures anonymity and makes it almost impossible to trace the user's footprints. This makes the Tor browser and dot onion web pages attractive for those wishing to maintain their privacy and secrecy.

IS in the Darknet

Indeed, anonymity does not mean that the darknet is a dangerous place. Individuals, especially journalists, use such avenues to hide themselves from prying eyes of authoritarian states and dictators. Similarly, Tor is used by those who wish to protect their privacy. However, illegal practices can and do happen because of the anonymity that is guaranteed by Tor and the darknet.

The darknet has provided criminals, non-state actors and terrorists tools and avenues that are absent in the surface net. For instance, a webpage by the name of 'Silk Road' functioned like the 'Amazon.com' for illegal activities, including the sale of drugs, weapons, fake passports and even hitmen. Criminals were comfortable dealing on this platform because of the anonymity in the darknet. The owner/founder of the Silk Road, Ross Ulbricht, was caught by FBI in 2013.

For IS and potential hackers, another attractive market in the dark net is that of hacking tools. IS and its United Cyber Caliphate has conducted several cyber-attacks in the last one year, usually in the form of defacing websites or hacking Twitter and Facebook accounts. The hacking tools and malware toolkits such as Keyloggers and Remote Access Trojans (RAT) are available in the darknet and it is highly probable that cyber terrorists and hackers download them from there.

Keylogger is a computer program that records every keystroke made by a computer user, while RAT is a malware program that enables administrative control over the target computer. As such, both are utilised to steal private and confidential

information. Even IS has attempted to distribute such tools amongst its 'cyber soldiers'. Additionally, IS hackers have also conducted cyberattacks such as the denial-of-service (DoS) attack, where a machine or service is made unavailable.

Islamic State is known for its innovations and ability to adapt to changing environments. When law enforcement agencies started snooping around social media, IS members, supporters and sympathisers migrated to mobile applications such as the WhatsApp and Telegram. The applications have become attractive modes of communication because of their end-to-end encryption, which prevents any 'peeping' by intelligence and law enforcement authorities.

Now a pro-IS deep web forum user has recommended that the group's users migrate to Tor and stop using VPN services, hence ensuring greater anonymity. The distribution of hacking tools also signifies IS' ambitions to expand its cyber capability. Considering the versatility of the group, this should not take too long.

Policy Implications

The 9/11 attack was the biggest terrorist attack which changed the complexion of global security. The American leadership and public never expected that an attack of this scale in a post-Cold War era could ever happen in the homeland. Yet, it did. Today, the attack that defined Bin Laden's notorious legacy seems less possible because of all the security measures and precautions that have been taken by countries around the world.

The lack of imagination before was the serious shortfall of security analysts and counter-terrorism specialists who failed to predict or even anticipate 9/11. If IS wants to surpass 9/11, it will conduct a cyber-9/11. This is not an impossible task considering the lax cybersecurity measures. The recent hacks of the Democratic National Committee emails and leaks to Wikileaks signify the vulnerability of private information. The DoS attacks by hacking groups such as Anonymous further underline the capacity of non-state actors to inflict damage.

Indeed, IS does not possess the capacity and capability to attack infrastructure as was the case with Stuxnet. However, even stealing information, hacking and denial-of-service attacks have serious implications. Furthermore, the loss in Syria and Iraq and the narrow space available to the group make a 'cyber caliphate' with hacking capabilities the most viable option and dangerous force.

A terrorist organisation that is anonymous and possesses an army of hackers is already becoming a reality. The world is increasingly becoming more connected via the Internet with government and private infrastructure heavily dependent on cyber technology. This is why, with or without IS, the next wave of terrorism is most likely to be 'cyber terrorism'. Rather than reacting to an attack in the future, the international community must pre-empt this threat now and take necessary steps.

Shahzeb Ali Rathore is a Research Analyst with the International Centre for Political Violence & Terrorism Research (ICPVTR), a constituent unit of the S. Rajaratnam

School of International Studies (RSIS), Nanyang Technological University, Singapore.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg