Cyber Terrorism an Emerging Threat to Sri Lanka's National Security

In the modern world, everything is digitalized. The world is accessible at our fingertips. Due to the wide accessibility, people tend to misuse technology. One such way is cybercrime. Cybercrime it is not a novel phenomenon in the world. Even though there are many definitions for cybercrimes, one common definition is for cybercrime is "*any criminal activity which takes place on or over the medium of computers or the internet or other technology recognized by the Information Technology Act.*" Cybercrime is a threat to national security. Cyber hackers can infiltrate security systems, disseminate false news, and spread hate speech, resulting in unrest in the community. This also affects detrimentally to international relations.

In the Sri Lankan context, several cyber-attacks happened in the past. The Liberation Tigers of Tamil Eelam (LTTE) hacked the government of Sri Lanka's websites several times. The new war utilized by; LTTE is Cyber-crime. Cyber terrorists are trying to control human behavior and the government's behavior using technology. With valuable information, anything can be dangerous if the information falls into a bad hand.

As Curran, Concannon, and McKeever (in Janczewski and Colarik 2008:03) point out, LTTE became the world's first terrorist group to attack a country's computer system in 1998. "In 1998, the LTTE organization immerse Sri Lankan embassies with 800 Emails a day for two weeks of the period. The message simply says. *"We are the Internet Black Tigers and we're doing this to interrupt your communications"*. Again, at the end of the fourth Eelam war, the LTTE launched an attack on several government websites. This time they were able to attack the Army website of the Sri Lankan government on 01st of May 2009. When considering these, LTTE's capability to carry out similar cyber-attacks and advanced cyber-attacks on the Sri Lankan government websites will prove their capability to use the new technology for creating trouble comprehensions on the rival's mind.

Nevertheless, it wasn't the end. LTTE cyber strategies got stronger than ever before. On 18th of May 2018, the organization called "Tamil Eelam Cyber Force", hacked the Sinhala version of the official website of the Ministry of Tourism Development and Christian Religious Affairs. Furthermore, they hacked the website of the Democratic Socialist Republic of Sri Lanka Honorary Consulate in Kerala. As a result of hacking, these websites displayed a long message from the Tamil Eelam Cyber Force and also a rolling news feed message which said *'Hacked by Tamil Eelam Cyber Force'.* Another attack has happened on the 6th of February 2021on the LK Domain registry. This cyber-attack investigation is still carried out by Sri Lanka Computer Emergency Readiness Team (SLCERT) along with the Information Technology Society of Sri Lanka (ITSSL). On 18th May 2021, the Chinese Embassy operating in Sri Lanka website, Ministry of Health website, Rajarata university website was affected by the cyberattacks. These cyber-attacks were also conducted by a group called "Tamil Eelam Cyber Force". Prime Minister Mahinda Rajapaksha's website was also hacked on the 3rd of June, 2021. ITSSL said the Prime Minister's website was hacked in a manner in which any visitor to the website would be redirected to another website that displays content related to Bitcoin Cryptocurrency. Due to all these website hackings, it questioned the security of data in government institutions.

The LTTE also uses various kinds of cyber strategies as an element of their War against the Sri Lankan state. According to "*Counter Cyber Terrorism Effectively: Are we ready to rumble*" by Shamsuddin Abdul Jalil, under the cyber strategy of LTTE, there were many things including, cyber-attacks, cyber threats, cyber propaganda, terrorist financing via the internet, and intense ideological and political campaigns against the Sri Lankan state. Additionally, the technological capability of the LTTE impelled the Government to be more concerned with its informational security.

Considering these facts, it appears that cyber terrorism is an emerging and existing threat in the country. Nevertheless, the challenge is, we cannot witness the threat from our own eyes. This is an invincible threat that we need to face carefully. As a country, we need to be aware of this matter more than ever. For that, we need to prevent and mitigate cyber terrorism. To do that, there should be a perfect strategy to follow. Such as,

- Increase the security awareness

Building awareness about cyber terrorism issues among the community is important. With proper education, they will realize the significance of defending themselves from similar attacks. It will also help to build more inventive communities dealing with information securities. Effective cyber security training programs can help people equip themselves with the skills and knowledge demanded to effectively cover their computer and network systems right.

- Stringent cyber laws

The government can help in controlling cyber-terrorist attacks by adopting new laws and revising prevailing cyber laws that will discipline the perpetrators more heavily if they are involved in similar conditioning.

- Implement cyber security educational policies

The government can implement effective educational programs and workshops with the collaboration of Computer Emergency Response Teams (CERTs), based in Sri Lanka, including Tech CERT, SLCERT to educate the citizens on e-literacy.

- Pursue and enforce the law against the perpetrators

The people, organizations, and governments who face cyber-attacks must enforce the law against the terrorists who carry out such attacks. Although this is a costly process, it allows us to accurately identify criminals and enforce the law. As a result, criminals will deter from committing crimes.

Even though cyber terrorism has become a new topic for most of us, it became a very challenging threat to the world. Government and the general public should work together to end this threat. So far, significant progress has been made through industry and government initiatives in many countries to protect against cyber-attacks. However, with the right strategic security measures, we can win this battle.

* *Mr. Thusitha Bulathgama is a Research Assistant at the Institute of National Security Studies (INSS), the premier think tank on National Security established under the Ministry of Defence. The opinion expressed is his own and not necessarily reflective of the institute.*