At TAHALOF

IMCTC Quarterly Magazine

Issue 3. May 2020

Terrorism in International Law


التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

At TAHALOF

Third issue, May 2020

IMCTC Quarterly Magazine

التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION
General Directorate of Planning and Coordination

Director General

Major General Mohammed bin Saeed Al-Moghedi

Secretary-General of the Islamic Military Counter-Terrorism Coalition

Editor-in-Chief

Colonel Hassan bin Suliman Al-Amri

Director of the General Directorate of Planning and Coordination

Brought to you by

TAOQ RESEARCH

TAOQ تـــوق

E-mail: info@taoqresearch.org

Phone: +966 114890124

For support and more information please contact the magazine editorial office

magazine@imctc.org

Digital Version

Pakistan experience of counterterrorism

4

NATO COUNTERTERRORISM STRATEGY

8

At TAHALOF

IMCTC Quarterly Magazine

ISLAMIC MILITARY COUNTER TERRORISM COALITION

General Directorate of Planning and Coordination

Third issue, May 2020

Publishing Policy

Terms and Conditions

• Disclaimer: The opinions expressed in this publication are those of the authors. They do not purport to reflect the opinions or views of the Magazine.

• The manuscript shall be within the scope of **At-TAHALOF** Magazine under the theme of counter-terrorism, and shall be pertinent to one of the four key IMCTC domains: ideology, communications, counter-terrorist financing and military.

• The manuscript shall be authentic, objective and novel, and shall be of a sound methodology, language and style.

• Research shall be well-referenced, sources shall be cited and a well-written list of references and bibliographies shall be provided.

• The manuscript shall be written in Arabic, English or French.

• Under no circumstances may the manuscript have been published by any formats even if minor or major changes are made.

• The manuscript either in whole or in part may not have been previously published or accepted for publication elsewhere whether by the same author or by a different author.

• The manuscript not accepted for publication does not mean such a manuscript is poor. Failure to obtain acceptance for such a manuscript may be due to technical or other

SENEGAL
COUNTERTERRORISM APPROACH

DRIVERS OF INTERNATIONAL COUNTERTERRORISM COOPERATION

THE THREAT OF CYBERTERRORISM AND THE APPLICABILITY OF THE CONVENTION OF CYBERCRIME

CAUSES OF TERRORISM INITIATIVE Al-Qaeda, ISIS and Boko Haram (Case Studies)

ISLAMOPHOBIA IN EUROPE
USING CRISES TO SPREAD HATE

considerations; for instance, the subject-matter of such an article has been addressed. The author of such an article shall be informed accordingly.

• The Editorial Board shall be entitled to adabt the manuscript submitted – including modification, editing, proofreading, tweaking, revising, conflation, truncation – without prejudice to the key ideas.

• A potential writer shall be entitled to republish his or her manuscript at his or her discretion, provided that he or she shall expressly state that such a manuscript has already been published in At-TAHALOF Magazine.

• At-TAHALOF Magazine shall be entitled to reproduce the manuscript in any formats, be it electronic or independent publications.

• At-TAHALOF Magazine shall be entitled to translate the manuscript into any language and republish such a manuscript in the language(s) desired.

• The manuscript shall be formatted, using Microsoft Word Processor in compliance with the following:

o Arabic:

Font Type: Traditional Arabic; Font Size: 18

o English & French:

Font Type: Times New Roman; Font Size: 14

Footnotes and sources, if any, should go at the end of the manuscript with font size (16) for Arabic and (12) for English and French.

• The Quranic verses of the Holy Quran shall be placed in parentheses and shall be appropriately cited, using the Ottoman calligraphy, with reference to the relevant verse and chapter numbers.

• It shall be desirable to attach illustrations relevant to the subject-matter; such illustrations shall be taken from specialized authentic resources rather than from newspapers and magazines.

• Attached to the manuscript shall be the author's curriculum vitae (CV), including: full name, nationality, country of residence, specialization, current job position, scientific and cultural publications, e-mail address, bank account number and a recent photograph.

DARK WEB OF TERRORISM

■ Mohammed Yazid bin Zu Qubali

Terrorists and extremist groups use the internet for the promotion of their ideology, glorification of terrorist acts, recruitment, broadcasting of violent content, facilitating communication and training potential recruits with anonymity. Online social networks are also used to spread their propaganda, fear, panic, intimidating messaging and threats to the public. Law enforcement agencies all over the world usually monitor and supervise the content of materials and communications in the cyber world to ensure that they are not used for illegal purposes. Unfortunately, criminals and terrorists have managed to bypass the supervision of law enforcement agencies by resorting to the dark web. To effectively counter terrorism and combat the financing of terrorism, law enforcement agencies must ensure that their officers are fully familiar with the state-of-the-art technology, spearheaded by the dark web.

Real Threat

The dark web can bypass censorship, supervision and monitoring of law enforcement agencies and can provide a higher level of anonymity to their users. Proper training and awareness campaigns are essential to ensure that all law enforcement agencies are fully equipped with know-how to handle the threats from the modern digital world – a real threat looming large. The emerging digital threats associated with the dark web, including cyberstalking, hacktivism, fraud, identity theft and attacks on critical infrastructure cannot be underestimated. The dark web, alternatively known as the deep web, is part of the internet that isn't indexed by search engines and is inaccessible by normal internet browsers. Since the materials on the deep web is not indexed, one should have the precise URL to access the page desired.

Unlike the normal use of the internet, in

■ Counterterrorism Consultant and Professor of Law at Ahmed Ibrahim Faculty, International Islamic University, Malaysia.

which the IP address of each computer or gadget can be detected straight away, the dark web can provide a higher level of anonymity to the users as the IP address of each computer or gadget accessing the dark web will be scrambled by using special browsers and networks like "The Onion Routing" (TOR) project and the "Invisible Internet Project". This special browser – TOR – was developed and funded by the United States Naval Research Laboratory in the 1990s as a tool for evading online detection with roughly 60% of its funding coming from the State Department and the Department of Defence.

The dark web allows people to purchase firearms, passports, driver's licenses and ID cards, healthcare data, credit card and social security numbers and pornography at relative ease. Due to anonymity, the dark web is also used to purchase stolen subscription credentials, hacked Netflix accounts and illegal software. The dark web also offers various illegal services, including assassination and hacking.

A global online marketplace in the dark web called the Silk Road once attracted over 100,000 users who transacted over one million deals, estimated to be worth $1.2 billion in global sales from vendors located in more than ten countries around the world before it was closed down by the authorities.

Flip Side

Not everything in the dark web is illegal. The dark web is simply an online platform neither regulated nor controlled. Since it provides anonymity, many people surfing the dark web feel that they can act with impunity because they will not be caught.

There is a legitimate side for the dark web, as well. There are various social clubs available on the dark web, including chess club and social networks similar to Facebook. Anonymous browsing also allows people in repressed countries to circumvent government censorship and avoid persecution for online activities and assist whistle-blowers who wish to disclose valuable information without compromising their identity.

The dark web encryption technology routes user data through a large number of intermediate servers, protecting user identity and providing anonymity. The transmitted information can be decrypted only by the next node (computer), which finally leads to the exit node. This makes it challenging to reproduce the node path as the information was encrypted layer to layer. Due to this advanced encryption, websites are unable to simply track and identify the IP address or GPS of their users, while users will not be able to track similar information about the host.

Confronting Threat

The general perception that the dark web provides complete anonymity is not entirely correct as technology exists to counter it. In a 2012 investigation entitled "Operation Torpedo," the Federal Bureau of Investigations (FBI) used a method called "Network Investigative Technique" to detect and identify the IP addresses of at least twenty-five individuals who have visited illegal websites on the dark web. To proceed with investigations relating to the dark web in the United States, the FBI can use the Network Investigative Technique (NIT) but a warrant is required. The NIT warrant authorized the FBI to deploy the NIT, which consisted of computer code that, when deployed to a user computer, caused such computer to send to a government computer its actual IP address.

One important question is whether accessing the dark web can be banned or not. The answer depends on the law of the country. In many countries, accessing the dark web, similar to accessing normal websites, is not illegal on its own. As mentioned before, similar to normal websites, the dark web also offers various legitimate services. However, accessing illegal websites that promote illegal services is contrary to law. This includes websites that offer illicit drugs, illegal services like hacking, malware and pornography. The law in most countries does not discriminate between the dark web and normal websites. Both are subjected to the same law although enforcement might be more challenging.

There are other challenges that share similar characteristics with the dark web. This includes Virtual Private Networks (VPN), proxy servers, anonymous e-mail providers, and other web services that neither retain nor provide any identification information. To address cyberterrorism threats, security agencies should always remain vigilant and provide adequate funding for staff, equipment, training, in addition to encouraging citizens to be alert and to report any suspicious behaviour.

It would also be very helpful if international coalitions such as the Islamic Military Counter Terrorism Coalition (IMCTC) can assist in developing a platform to coordinate such training and technology sharing for counter-terrorism purposes in the future.

At TAHALOF

IMCTC Quarterly Magazine

التحالف الإسلامي العسكري لمحاربة الإرهاب

ISLAMIC MILITARY COUNTER TERRORISM COALITION

General Directorate of Planning and Coordination