

# التحالف

ALLIED: MONTHLY BULLETIN ISSUED BY IMCTC

## WAR COLLEGE STUDENTS VISIT IMCTC



Several students of the War College in Riyadh (Cohort 12) visited IMCTC, April 6, 2021, and were introduced to the IMCTC departments and sections. The delegation was provided with a background of the IMCTC goals and initiatives, expressing their appreciation for the robust engagement made by IMCTC in coordinating the efforts of the IMCTC member countries in countering terrorism, combating extremism and supporting international peace and security. 🌸

## RECEPTION OF DELEGATE OF YEMEN FAREWELL TO DELEGATE OF SUDAN



IMCTC received Lieutenant-Colonel Fahd Ahmed Saeed Ali, Delegate of the Republic of Yemen to IMCTC, who assumed his duties at the IMCTC headquarters, April 6, 2021, among other delegates of the IMCTC member countries. In a similar vein, IMCTC bid farewell to Brigadier General Musa Omar Ahmed Saeed, Delegate of the Republic of the Sudan, April 7, 2021. 🌸

# INDICATORS OF RELIGIOUS EXTREMISM HIGHLIGHTED BY KEYNOTE LECTURE AT IMCTC CENTER



Riyadh, April 5 of 2021

**IMCTC** held a keynote lecture, featuring Indicators of Religious Extremism by Dr. Abdul-Rahman Mohammed Asiri, Professor of Sociology at Imam Muhammad bin Saud Islamic University in Riyadh, Professor of Prince Nayef Chair for National Unity Studies. Professor Asiri provided an analysis of the social, economic, psychological, appearance, religious, and political indicators of violent extremism subject to monitoring.

## Disparity and Difference

Professor Asiri stressed the importance of identifying the type of extremism to better identify relevant indicators. Extremism per se is a relative issue, varying through time and place. He spelled out that we do not have specific and scholarly unanimous indicators for ideological or religious extremists. Research studies reveal indicators following analyses of myriad cases, supported by scholarly reports that examine the conditions of some extremists, whether in terms of behavioral signs or methods of affiliation with these groups or contributory factors.

However, such indicators cannot be viewed as fixed and general for ideological and religious extremists in all communities and times; they differ according to gender, as males show signs of extremism not evinced among females. Different ages, family characteristics and duration. In the past, an ideological extremist used to go through a relatively long and gradual phase until some observable indicators came visibly into play; while, the transformation is currently taking place in a few days, rendering the family helpless to observe any changes in any family members that suggest extremism.

## Social Indicators

This indicator is one of the strongest indications of extremism. As a person's desire to shut oneself off in one's own room, it is an indication that the person has something to hide from his family. If this is a family emergency, then it is a strong indication of the person's involvement. This situation has become a big problem today among most families, after the emergence of so-called hotel-like families. This makes the family less interested in this indicator! With children being shut off in their rooms, most families have been consumed by this vexing dilemma. Such behaviors are akin to playing truant from school and ceasing to participate in recreational activities. This indicator has been commonly observed in many families, manifested in avoiding engagement in playing

sports clubs, practicing some hobbies and severing previous relations with new peers sneaking into an extremist's life for the first time.

Among the social indicators of extremism is the extremist's use of violence with those around them, especially their families on the pretext of changing evil! Studies have examined this indicator in a large number of cases, revealing a sudden change in their vehemence to prohibit, smashing some tools that they deem forbidden, such as television and musical instruments, or they prevent the family from using such tools, and they may force them to watch specific channels only alongside excessive guardianship of women, sisters and wives.

One of the most important social indicators of extremism is also being absent from home and concocting excuses, such as traveling with peers or otherwise; this becomes glaringly noticeable at the beginning of one's embrace of extremism. Such a person hides from his family his contact or affiliation with extremist groups. It has been observed among many of those who are ideological extremists with their lack of engagement in social events, their lack of family socialization, their frequent travels and the desire to go out with new peers on road trips.

## Economic Indicators

The economic indicator is one of the most important traditional indicators that show the extremist's deviation from the path of righteousness, rectitude and truth, including the person suddenly turning to charitable societies and volunteering in them with the aim of fundraising and pooling financial or in-kind donations from businessmen and the public, decoyed as charitable work, or preparation of the invader, or jihad or otherwise expressed to fund suspicious activities and organizations.

A telling indicator is a person that has suddenly left his government job and turned to easy trade, such as selling vegetables, honey, dates, perfumes and incense, justifying that on suspicions related to the legitimacy of government work. Among the economic indicators is the change in the financial position of the extremist, negatively or positively, either by his loss of money without a sound justification, or by his suddenly amassed wealth and unusual spending.

## Mental Indicators

One of the most prominent mental indicators of extremism is the extremist's isolation and alienation from those around, staying

away for long hours, browsing the websites of extremist groups and terrorist organizations or evincing engagement. A person's frequent visits to websites of extremist and terrorist groups, or showing engagement can be a strong indication of his attraction to the ideology of such groups and organizations. Unfortunately, this is difficult for the family to discover but easy for security authorities.

Signs of distress, anxiety and depression are felt by an extremist when mentioning the security services and terrorist crimes, expressing constant suspicion of everything.

### Appearance Indicators

Extremists tend to change their appearance as their ideas change. Therefore, one of the appearance indicators of extremism is the glaringly stark difference in the appearance of an extremist, especially clothing. Some dress in Afghani costume, unusual colored headdresses and turbans (brown, gray, and green), or the black hood known as (the Zarqawi hat). They display strange behaviors, such as extending the beard and hair too much, shaving the entire head of hair, or leaving a good-looking appearance as an expression of austerity.

### Religious Indicators

This is displayed by religious extremism, intolerance, exaggeration in contradicting moderation of Islam and tolerance of Sharia, misunderstanding of religious scriptures, misinterpretation of the Noble Quran or hadiths whimsically, or being too literal and brushing aside the core meaning, turning a blind eye to their aims and objectives. Among the most notorious telling instances is the erroneous interpretation of the jurisprudence of the Imams Ibn Taymiyyah and Ibn Al-Qayyim and their opinions, citing and quoting them inappropriately.

Likewise, excluding the followers of other religions, the rejection of the other opinion, the unwillingness of dialogue, the superiority over those around on the pretext that they are among the people of deviation and immorality or among the people of heresy and misguidance, drumming up their spurious belief that others are disbelievers, misguided or infidels, especially the rulers and scholars, while stigmatizing the scholars and calling them the Sheikhs of the Court.

Among the indicators that have been observed among the extremists, especially in the early stages of extremism, is their isolation from the congregational services and abandonment of prayer in mosques. This may be part of their feeling of apostasy and infidelity of the worshipers, and the inadmissibility of prayer with them. It may happen when the extremist's religiosity is sudden, and he goes to the mosque for repentance and forgiveness. Also among the religious indicators is the desire for leadership of the person

who is ideologically affiliated with any of the extremist groups or terrorist organizations, and the attempt to appear as a preaching sheikh or imam who should be emulated. If he is in a group and it is high time for prayer, then he rushes forward to lead the worshippers, even if he is not requested to do so, even if others are more knowledgeable and well-rounded in leading worshippers and older than him; he is deceived by his feeling of being elevated and sublime.

Among the indicators of this type is when a person speaks highly of the suicide operations carried out by terrorists, calling them martyrdom operations, denying the geographic and political borders of countries due to the belief in what he calls belief-based affiliation.

The same applies to holding onto dignities, clairvoyancy, prognostication and dreams, believing and drumming up for them. This was employed strongly during the Afghanistan war, and it became one of the common beliefs among the fighters at that time. It is still one of the indicators in which many extremists believe to deceive and decoy others.

### Political Indicators

It is a strong indication of a person who has reached an advanced stage in adopting the ideology of terrorist organizations, overcoming the latency stage and moving up to the stage of emergence, lack of fear and the transition to the stage of openness, such as participation in demonstrations organized by extremist groups or sympathy and support for them. It was observed in some national and international events. Extremists actually participated or put up the logo of specific organizations, or they broadcast images or footages of events that they considered a victory for those oppressed, using the symbols and signs of extremist and terrorist organizations.

Among the political indicators is the underestimation of scholars, statesmen, and others, who oppose the ideology of extremism and militancy. This gained prominence at a stage known as the awakening that was rooted for negative criticism of those who opposed their ideology. This behavior continued among those who embraced the ideology of the Kharijites, as an extension of those religious parties. In exchange for the disparagement of scholars, extremists praise the symbols of extremism and terrorism, and describe them with political or religious titles, such as Caliph, Commander of Believers, Mujahid, Sheikh, Imam, and the like.

Conspiracy theories are embraced by this type of extremists, as they see that the Muslim world is subjected to conspiracies by other nations, especially the West. Therefore, they take a position hostile to such nations, and everyone who contradicts them and calls for tolerance is looked down at as secular or liberal, thus their narrative divides people into us and them. ❁



# METHODS OF CYBERATTACKS HIGHLIGHTED IN IMCTC KEYNOTE LECTURE



**IMCTC** in Riyadh held a keynote lecture on “Methods of Cyberattacks,” on 7 April, 2021, which is part of a lecture series termed conscious, by Dr. Sultan Dawood Al-Farhoud, Assistant Professor at King Saud University. Dr. Al-Farhoud discussed data security practices, types of cyberattacks and protection methods.

Dr. Al-Farhoud highlighted the latest major cyberattacks. On March 18, 2021, Google published detailed information on one of the most sophisticated cyberattacks conducted by one country, and revealed a platform to penetrate various systems in Windows, IOS and Android. Dr. Al-Farhoud pointed out that information security aims to achieve confidentiality and ensure continued flow of information, valid and accurate content, given the cyberattacks that government and private institutions and individuals sustain; 70% of such cyberattacks are conducted by foreign parties, 55% by organized crime groups, and 30 % by saboteurs from within. While they all seek to achieve financial, ideological, political, personal or moral goals, more than 86% of the cyberattacks were financially motivated and 10% were driven by espionage.

## Substantial Losses

Dr. Al-Farhoud warns off that cybercrime will cost the world \$ 10.5 trillion per year by 2025, and every minute the world loses 2.9 million dollars because of cyberattacks. The average cost of a data breach was \$ 3.66 million in 2020. Dr. Al-Farhoud provided an analysis of the most notorious attacks, such as the 2017 Wanna Cry Attack, which was a malware program that encrypted the contents of computers, requested ransoms to recover data, attacked 200,000 computers in 150 countries and inflicted losses

estimated at about four billion dollars. The attack on Twitter in 2020 targeted 130 important accounts, including those of former presidents of the United States of America and Elon Musk. The attack on Twitter is often based on identifying the victim through a fake phone call or a fake VPN, then stealing access data to the systems and stealing information. SolarWinds has been penetrated by a cyberattack that reached its customers; it was not discovered throughout 2020.

The attackers were able to spy on private companies such as Microsoft and FireEye, and infiltrated the systems through a malware code, bringing damage to more than 33,000 customers (of whom 18,000 have received malware). Opening a back door to the IT systems through a malware code, the attackers installed more spyware malware programs. The attackers penetrated more than a few important departments of the US government, including the Department of Defense, the Department of Homeland Security and the Treasury.

The COVID-19 pandemic was a favorable opportunity for hackers and attackers to increase cyberattacks; the attacks on cloud systems increased by 630% between January and April 2020, and they increased by 238% on banks in 2020, and half a million accounts were compromised in the Zoom application in April 2020. When COVID-19 pandemic broke out, 27% of cyberattacks have targeted banks or healthcare institutions.

## Modalities of Cyberattacks

Dr. Al-Farhoud reviewed the modalities of cyberattacks, including malware, social engineering, spam, denial of service attacks and

advanced system penetration. He also remarked that 45% of the cyberattacks involved attempts to penetrate systems, of which 17% involved malware and 22% are phishing. Prime examples of the most notorious advanced penetration methods include SQL Injection, Cross Site Scripting (XSS) and Man-in-the-Middle.

**Malware Programs:** They include viruses, spyware, ransomware, and adware. Crypto-virology is used by attackers by exploiting storage media, email, malware software, or suspicious websites. Dr. Al-Farhoud confirmed that in 2018, about 10,573 malicious mobile phone applications were blocked per day, and the average payments for ransomware requesting software increased in 2020 to reach \$ 111,605, an increase of 33% compared to that of 2019.

**Social Engineering:** This is one of the most successful and easiest means of penetration; it is used in 98% of cyberattacks, in which the attacker deceives and decoys the user to willingly reveal confidential information or enable him to access confidential information, whether by phone, via e-mail or social networks. Social engineering does not depend on deep technical knowledge, so anyone with know-how or savvy can do it; a message claiming to be from the administration of an application or program that a potential victim uses may reach the victim, informing him that his request has been processed, requesting him to enter the link attached thereby. It is a malware software program that infiltrates one's device and hacks one's data.

A message may arrive to a guest user in a hotel claiming to be from the hotel's management, informing him that there is an error in the credit card information with which he paid for the reservation, requesting him for card information; the contact is not from the hotel; rather, from a person who follows up the hotel's guests when they come to surreptitiously contact them, to hack and steal their credit card data. You may receive a message saying: "Register your data to participate in a prize draw opportunity," which is a ploy to hack your device. Social engineering methods often pay off because attackers exploit rumors and hot topics, feed on the good reputation of certain applications, and the user's poor technical expertise, especially those who use weak passwords.

**Phishing:** It is one of the types of electronic attacks; attackers attempt to obtain sensitive information, such as usernames and passwords, disguised as a trustworthy entity in electronic communication. In 2019, 88% of organizations worldwide were exposed to phishing attempts.

Attackers use unwanted messages sent electronically without the user's request. The number of electronic messages of this type reached about 14.5 billion messages per day, accounting for 45% of the total emails.

Among the most dangerous cyberattacks are denial of service that floods systems with unnecessary data that infects devices with programs that attackers can control remotely, and send such data to the systems intensively. This causes these systems to be slow to respond to the demands of their users.

### Protection and Prevention Methods

In conclusion, Dr. Al-Farhoud highlighted that information security practices are based on three pillars:

**First:** prevention can be realized by taking measures to protect the data from damage or theft.

**Second:** discovery can be realized by implementing procedures to detect leakage or corruption of data and uncover the perpetrator and the causes.

**Third:** treatment can be realized by taking measures to contain cyberattacks and reduce their impact.

The data protection methods can be individual and institutional. The most important individual protection methods include:


- Use strong passwords. Using the largest number of letters, numbers and symbols, while avoiding using one password in all sites, changing the password every time, and using two-step verification methods.
- Always update the software and the operating system, and download all necessary updates when released.
- Mobile and unreliable storage media is not used to store confidential data.
- Use safe methods to dispose of data because removing it by traditional methods does not mean getting rid of it permanently. Data can be retrieved using special programs and tools.
- Beware of opening attachments and links before verifying and trusting them. Among the most harmful e-mail attachments are .doc and .dot, which are spread by 37%, and .exe that is spread by 19.5%.
- Beware of using untrusted computers.
- Use anti-virus and anti-hacking programs.

Among the institutional protection methods are those relating to employees and information technology officials. The employees must adhere to the aforementioned protection methods related to individuals, and it is critically important not to share access data to the systems, and not to browse websites unrelated to work.

Information technology officials in institutions should bear a responsibility to protect information. To this effect, they can use many methods that increase what ordinary individuals or employees follow. The most important methods include:

- Check for recent backups of important information and files.
- Limit the number of employees and specialists who have accounts that have systems management authority over the institutional networks, systems and applications, and verify the employee's need for these powers.
- Record all operations that they perform using accounts and always check them.
- Review logins and unsuccessful attempts on servers and devices with systems administration authority.
- Remind professionals not to use systems management accounts to read e-mails, view attachments or browse the Internet.
- Use of firewall and encryption.
- Detect and prevent intrusions in networks, fix vulnerabilities and control access.

Combat malware on servers.

- Verify entries in applications, assessment of vulnerabilities and access control.
- Data encryption and access control. 

# THE SYMBIOTIC RELATIONSHIP BETWEEN TERRORISM AND TRAFFICKING

## TERRORIST GROUPS AND CRIME NETWORKS EVINCE COOPERATION AND INTERDEPENDENCE



**Colonel** Roger Nikapisse, Delegate of the Gabonese Republic to IMCTC in Riyadh, presented a keynote lecture, Sunday April 11 of 2021, featuring "The Symbiotic Relationship Between Terrorism and Trafficking." Nikapisse provided an analysis of how terrorism and trafficking are linked together, the methods used by terrorist organizations in managing their finance and the sites preferred for their trafficking practices, the key contraband goods, the impact of the synergic relationship between terrorism and trafficking in the counterterrorism areas adopted by IMCTC and measures that should be taken to delink terrorism and trafficking.

### Different Objectives

Nikapisse initially emphasized that terrorism and trafficking are two notorious threats all over the world, which have exacerbated the vulnerability and lack of security in countries and communities, increased the risks of instability and undermined development efforts. Taken together, the links between terrorist groups and cross-border trafficking networks have become stronger, aided by cooperation and interdependence. As reported by INTERPOL, the illicit financial flows resulting from such activities in 2018 in the conflict areas and beyond were estimated at about \$ 31.5 billion.

If traffickers are seeking economic and financial gains, then such terrorist organizations adopt a different logic of their involvement in trafficking practices; they funnel funds to finance terrorist activities, driven by ideological, doctrinal and political goals.

Since the restrictions placed on terrorist financing sources, especially after the 9/11 Attacks of 2001 alongside the imposition

of international sanctions targeting sources of funding, within the framework of the United Nations, terrorist organizations have abandoned the traditional banking sector and resorted to concealed transactions. In this context, they adopted a strategy of self-financing and independence to reduce their political and ideological dependence on state or individual donors. This strategy is evident in the logic of decentralization of terrorist cells. They are encouraged to finance themselves. Today, such terrorist cells operate in the shadow, exploiting loopholes in the national and regional legal systems. These facts proved the interdependence and interrelation between terrorist and criminal circles, nurturing a new generation of traffickers in terrorism. Unsurprisingly, the Security Council issued Resolution 1373, which recognizes the interdependence between international terrorism and transnational organized crime.

### Financial Needs

Nikapis provided an analysis of the financial needs of terrorist organizations to achieve their goals, whether carrying out their terrorist attacks, recruiting and training fighters, or obtaining the appropriate technical means and ensuring propaganda. This also includes daily life provision of food, shelter, travel for communication, recruitment, consultation, instructions, use of intermediaries and the maintenance of network.

To meet these financial needs, terrorist organizations such as ISIS adopted the method based on widespread looting in the areas they controlled. They have also carried out their activities as if they

were real commercial institutions keen on investing in local and legal economies, especially in areas where states are weak, which is a stepping stone to further control other areas in the future to achieve the maximum gains in terms of financial resources. These are investments that would strengthen the relations of such organizations with communities and increase their influence in the areas under their control.

An analysis of the attacks carried out in recent years in Europe revealed that the attackers would finance themselves in various trafficking operations, and that 95% of the perpetrators of recent terrorist attacks in Europe had functional experience as fledging yet apprenticed criminals.

### Favorite Sites

Nikapisse indicated that trafficking activities are limited to poorly state-controlled areas and areas caught in the poverty trap. Given the vulnerable states and the uncontrollability of large swaths of territory and the porous borders, criminal groups snowballed and slithered away into these places, where the multifaceted networks of illicit trafficking are linked to cross-border crimes, turning such areas into a breeding ground and making trafficking practices sprout up especially drugs, ivory trade and illegal immigration.

Residents in the borderline areas take advantage of the ease of penetration of the borders to engage in illegal activities with networks on both sides, selling contraband goods fraudulently. This helps the population isolated in these areas to obtain basic low-price goods, not provided by the government. The economies of these borderline regions gradually separate from the national economic circles, merging into transnational circles dominated by traffickers. Social sympathy is felt towards such trafficking activities in which many citizens in these areas consider it innocent trafficking and rarely do they see it as a criminal activity.

Areas of conflict and instability are a breeding ground for an alliance between criminal groups and terrorist organizations, undermining peace and stability. Terrorist groups and criminal trafficking networks can share places to control roads and various economic axes, in vast cross-border areas, linked to the globalization of organized crime. In these areas, the threat of real collusion between terrorism and organized crime becomes glaringly insidious. If the convoys of illegal contraband products crossing the regions are under the protection of terrorist groups, the businesspeople pay a percentage of the value of the trafficked contraband goods.

### Contraband Goods

Nikapisse cited several telling instances of contraband goods used by terrorist organizations, explaining that the contraband materials vary widely, including drugs, oil, smoke (cigarettes), counterfeit medicines, firearms, ammunition, antique crafts, metals and other natural resources. The United Nations Office on Drugs and Crime (UNODC) estimated these illegal flows, in 2009, at about \$ 3.8 billion, for West Africa alone.

Some terrorist organizations specialized in producing or exporting narcotic drugs. The Naples Police Department in Italy, on July 1 of 2020, seized the largest shipment of amphetamines in the world (14 tons), including 84 million Captagon tablets produced by DAESH in Syria. DAESH fighters use this drug to dampen their fear and make them very aggressive.

Oil smuggling is increasingly growing in conflict-fueled areas; it is a source of funding for terrorist organizations, or those associated with organized crime. The global volume of smuggled oil every year is estimated at about \$ 133 billion. The illicit sale of oil for

the benefit of DAESH, after its control of several oil fields in Iraq and Syria, was one of its main sources of income, estimated at two million euros per day.

Contraband cigarettes represent more than 20% of the criminal sources of financing terrorist organizations as revealed by a report issued in 2015 by the Center for Terrorism Analysis. Among these organizations are Hezbollah and Al-Qaeda in the Islamic Maghreb, whose leader Mukhtar Belmokhtar made a notorious engagement in this illegal activity in the Sahel, and was thus dubbed Mr. Marlborough.

Illicit ivory trade has also become a source of income for the head of the Lord's Resistance Army (LRA), which is active in the border triangle between South Sudan, Central Africa and the Democratic Republic of the Congo. As estimated, the armed groups south of the Sahara receive an income of 4 to 12.2 million dollars, whose trade volume reaches 3 billion dollars per year, despite the ban placed since 1989.

Terrorist organizations and organized crime groups resort to the illicit trade in firearms, which contributes to instability. In 2006, experts estimated the number of light weapons in circulation in the world from illicit brokering activities in conflict areas at more than \$ 600 million.

### Impact and Solution

Nikapisse explained the impact of the parasitical relationship between terrorism and trafficking in the IMCTC counterterrorism areas of action: ideology, communications, counter-terrorist financing and military domains, which are the areas that IMCTC attaches great significance to:

- ▶ **Ideology Domain:** trafficking or smuggling provides the necessary resources to support the financing of terrorist ideology.
- ▶ **Communications Domain:** The financial capacity gained through trafficking or smuggling helps terrorist groups to acquire modern media outlets that suit their ambitions.
- ▶ **Counter-Terrorist Financing Domain:** the financial flows generated from trafficking activity provide terrorist organizations with financial self-sufficiency and independence, and guarantee their ability to operate.
- ▶ **Military Domain:** trafficking provides an opportunity for terrorist organizations to enhance their ability to operate by acquiring equipment and machines, including weapons and ammunition.

In conclusion, Nikapisse called for the development of a set of initiatives to delink terrorism and trafficking. At the national level, Nikapisse called for the restoration of state authority, putting an end to the illegal exploitation of natural resources by securing national human and service capabilities aimed at enabling control over territory, especially borderline areas, enacting laws to combat organized crime and terrorism that address potential gaps in the applicable statutory provisions.

At the regional level, security and judicial cooperation between countries must be further strengthened, ensuring that intelligence information is shared with the aim of tracking down traffickers and dismantling criminal networks.

At the international level, coordination of cooperation in the face of terrorist threats must be strengthened, and the United Nations should continue to support countries and regional organizations to enhance their combat capabilities in various fields, especially intelligence, security, and judicial cooperation. 🌀

# TERRORIST FINANCING SOURCES AND COUNTERMEASURES HIGHLIGHTED IN IMCTC



Colonel Ali Mohammed Mahmoud, Delegate of the Kingdom of Bahrain, Colonel Ibrahim Musa, Delegate of the Republic of Niger and Mr. Khaled Arab, Delegate of the Islamic Republic of Afghanistan, presented a symposium, featuring “Sources of Financing Terrorism and Countermeasures,” sponsored and organized by IMCTC in Riyadh, April 21 of 2021.

The symposium addressed the definition of terrorist financing and life cycle, the triggers of terrorism and associations to financing operations, the three principles of combating terrorist financing, which are United Nations resolutions and agreements, recommendations of the Financial Action Task Force (FATF) and similar regional bodies, and an efficient counterterrorism system based on a legal and regulatory framework. It also addressed the challenges facing combating terrorist financing and provided recommendations.

## Threat of Terrorist Financing

Colonel Mahmoud first explained the threat of financing terrorist groups, highlighting the importance of combating terrorist financing. He spelled out that financing terrorism is one of the triggers of terrorism, as it is the lifeline for survival. Each and every stage of a terrorist action needs funding, which allows terrorists to always plan and implement violent extremist operations; they are in urgent need of funding at the strategic, operational and tactical levels. Therefore, any funding cut is a fatal blow to terrorism and terrorists. Combating terrorist financing is an important course of action for IMCTC, and a major means of curbing terrorism. It is a pathway that can be implemented remotely, without direct confrontation with terrorists or bloodshed.

Colonel Mahmoud provided a procedural definition of terrorist financing: any act committed by an individual or group, by any direct or indirect means, to collect, manage and spend funds for the purpose of terrorism, whether intentionally or unintentionally. Money laundering is any activity by individuals or groups to transfer funds related to crime, or funnel such funds intentionally or unintentionally to conceal original source.

## Terrorist Financing Cycle

Colonel Musa explained that the terrorist financing cycle begins with collecting funds from legitimate and illegal sources, depositing and transferring such funds, whether as intangible funds or precious stones, then concealing the source of such funds to finance operations, recruitment and social support. In the early cycle stages, the actions of terrorist organizations intersect with the actions of transnational organized crime groups, evidenced across the world, as is the case in Africa and Latin America.

Colonel Musa provided an in-depth analysis of the triggers of terrorism and association with financing. He further explained that terrorist activity feeds on three main factors: operations that need services, support that needs human and logistical resources and development that needs change, growth and transformation. Funding comes into play as *raison d'être* for existence and continuity in all these operations and requirements.

## Combating Terrorist Financing

Mr. Arab presented the principles of combating terrorist financing, spearheaded by the United Nations treaties and resolutions of Anti-Money Laundering and Counter-Terrorist Financing Rules,



the recommendations of the FATF and an efficient system for combating money laundering and terrorist financing. The United Nations has issued several relevant key resolutions, including the following:

1. United Nations Security Council Resolution 1267, October 15 of 1999, regarding Al-Qaeda and the Taliban Movement, established a Security Council committee to impose air embargoes and financial blockades on the two organizations, and the individuals and entities associated with them, and supervise the implementation of the penalties provided for in the resolution regarding the two organizations. The resolution was issued under Chapter VII of the United Nations Charter; it requires all countries to freeze the financial assets of individuals and entities belonging to or associated with the two organizations.

2. United Nations Security Council Resolution No. 1373, which the Council states unanimously adopted on September 28 of 2001; it aimed at disrupting terrorist groups by all means, and encouraging UN member states to share intelligence information on these groups to help fight international terrorism. It also called on all states to amend their national laws to ratify all existing international conventions on terrorism. The resolution established the Security Council Counter-Terrorism Committee to monitor compliance with relevant provisions.

The Committee issued the technical guide to implement the resolution, including the necessary preventive measures to be taken by financial institutions and businesses to combat money laundering and terrorist financing, and approaches to counter alternative transfer systems, such as hawala and money transfer services.

3. United Nations Security Council Resolution 1617, issued on July 29 of 2005, provided that all states shall take the measures previously imposed by resolutions 1267 in 1999, 1333 in 2000, and 1390 in 2002 relating to freezing the assets of terrorist groups, and the period for each and every penalty imposed on Al-Qaeda, its leader, Osama bin Laden, the Taliban, and their followers by travel ban, and the ban on supplying them with weapons. The Security Council urged all members of the United Nations to apply the comprehensive international standards contained in the relevant recommendations of the FATF related to anti-money laundering and combating terrorist financing.

4. United Nations Security Council Resolution No. 1988, June 17 of 2011, targeted the Taliban Movement and affiliated groups, institutions, entities and individuals by freezing their funds, financial assets and economic resources, preventing their entry to the territories of the UN member states and preventing the supply of weapons to them.

The most important international agreements and treaties that addressed combating terrorist financing include the following:

- ▶ The United Nations Convention against Illicit Trade in Narcotic Drugs and Psychotropic Substances in 1988, known as the Vienna Convention.
- ▶ The International Convention for the Suppression of the Financing of Terrorism, adopted by the United Nations General Assembly Resolution No. 54/109, December 9 of 1999. It is the most important international agreement to combat terrorist financing. It has precisely defined the crime of financing terrorism, associated elements, and what is meant by the funds and proceeds in financing terrorism.
- ▶ United Nations Convention of 2000 to combat transnational organized crime, known as the Palermo Convention, which is broader than the Vienna Convention because it provides for

all the proceeds of organized crime, and is not limited to drug trafficking; it criminalizes the laundering of the proceeds of such crimes, and imposes anti-money laundry measures.

## FATF and Affiliates

The FATF is an intergovernmental body established in 1989 and is based in Paris, France. It seeks to set global standards for anti-money laundering and combating terrorist financing. The group developed forty FATF recommendations for anti-money laundering and combating terrorist financing; the first of which was issued in 1989 and the last one in 2012.

The recommendations were divided into seven chapters, each of which addresses a specific aspect. Nine regional bodies have been established, such as the Financial Action Task Force (FSRBs), which together with the working group form a global network to combat money laundering and terrorist financing, evaluate member states' compliance, enhance international cooperation and provide technical assistance to member countries.

## Anti-Financing System

Mr. Arab provided an analysis for the elements of an effective anti-money laundering and combating terrorist financing system to effectively carry out the processes of prevention, suspension, detection, freezing, seizure and confiscation:

1. **Good Legal and Regulatory Framework:** it allows solid cooperation between the relevant authorities to work in a timely and efficient manner to control, freeze and confiscate terrorists' assets and financial returns, criminalize money laundering and terrorist financing operations and impose preventive regulatory conditions on financial and commercial institutions.
2. **Financial Intelligence Units:** the central agency for receiving, analyzing and disseminating financial information is a major destination for domestic and international cooperation.
3. **International Cooperation:** this helps in ratifying and implementing international agreements, and compliance with the FATF recommendations to facilitate mutual legal assistance and build comprehensive and meaningful local capacity.

## Challenges and Recommendations

Colonel Musa reviewed the challenges facing the fight against terrorist financing. The most notorious are the difficulties of controlling intangible operations, monitoring the change of terrorist organizations to their methods of money laundering and counter-measures.

This also included the exploitation of such organizations for technical progress in achieving subversive goals, and the failure of many countries to implement the FATF recommendations as revealed by the follow-up reports given the weak potential. Colonel Musa made several recommendations:

- ▶ Collective response in combating terrorist financing.
- ▶ Awareness of tracing processes for new financing methods.
- ▶ Compliance with UN resolutions, international treaties, and FATF recommendations.
- ▶ Strengthening programs to build the capacity of the competent authorities in anti-money laundering and combating the financing of terrorism.
- ▶ Domestic and international cooperation in sharing information and legal aid. 

## SMALL-DOLLAR TERRORISM IS ADDRESSED BY ISSUE (7) OF AT-TAHALOF MAGAZINE



The seventh issue of At-Tahalof Magazine came out, May 1 of 2021, featuring seminal reports, analyses, discussions and research addressing various aspects of terrorism and monitoring associated transformations. The current issue turns the spotlight on small-dollar terrorism as a last-chance strategy for terrorist organizations, given the pressures and defeats they face. Such organizations resorted to low-cost and available means, such as stabbing, setting fires, vehicle ramming and small improvised bombs. Such methods create more opportunities for terrorists to launch dangerous attacks, with minimal cost, training, and previous experience. After 2008, the rate of using knives in terrorist attacks rose to 33% vis-à-vis 7.3% between 2001-2007.

Terrorists found knives, vehicles, and inexpensive bombs made from materials sold in markets appropriate tools to further carry out criminal operations. The strategic estimates almost unanimously agree that the most persistent terrorist threats will come from decentralized terrorist cells, which carry out attacks of this type of terrorism, after the major terrorist attacks became very difficult.

Brigadier General Nawaf Nasser Al-Jetaili explained the reasons why terrorist organizations resort to low-cost operations and consider them as their last resort. He spelled out that such reasons include poor economy, defunct and moribund organizations, tight security measures, lack of time, individual behavior and a well-designed plan that reduces costs. He explained the impact and risks of such operations, characteristics and advantages, providing solutions for protection and prevention at the national and international levels.

Mr. Ashour Al-Juhani addressed the critically large gap between the costs of terrorist action and the counterterrorism costs. While the cost of carrying out any suicide attack, whether by bombing or indiscriminate shooting, does not exceed \$ 150, this small amount causes the global average of 12 deaths and spreads terror among hundreds of people. In contrast, the cost of the tight security measures imposed on vital places around the world to prevent terrorist operations amounted to more than \$ 300 billion. The low-cost means of terrorism that terrorist organizations have used on the institutions for combating terrorist financing, spearheaded by the Financial Action Task Force (FATF), have posed a new challenge to confront microfinance, while law enforcement and financial institutions developed methods of detection in anti-money laundering and combating terrorist financing on a large scale, regulations and procedures remain designed to thwart only large flows of money to terrorist organizations.

Dr. Salim Farrar provided an analysis of the efficiency of the financial and legal instruments in implementing the laws of combating terrorist financing. If many countries apply mandatory reporting on all financial transactions that exceed ten thousand dollars or equivalent, then many cases of small-dollar terrorism involve much lower amounts. Tracking small amounts will involve a very large number of transactions, be very costly to enforce and undoubtedly involve many innocent people.

Mr. Mahmoud Al-Hamdan highlighted the challenges of small-dollar terrorism triggered by the ease of access to such tools alongside the severity of the lethality created,

which made small, light and low-cost weapons easily made accessible and the preferred weapon for many terrorist groups around the world, given the poor international response in combating illicit trafficking of such weapons.

Meili Criezis discussed the strategy of terrorists in facilitating their actions by resorting to the types of terrorism that are most effective in achieving their goals, without the need for substantial expertise or huge financial investment, after the internet made available materials and instructional guides and a variety of low-cost attack ideas, coupled with publicity and temptation to extremists, supporters of terrorist groups and sympathizers.

The author reviewed extremist propaganda that promotes terrorist plans and methods with a low budget, and how extremists and terrorists recycle these plans and methods to implement their extremist ideologies.

### The Arab League and Counterterrorism

In the section (Strategies), Dr. Mazen Shandab provided a critical analytical reading of the Arab League Counterterrorism Strategy, reviewing the situations of the Arab League counterterrorism efforts, spearheaded by the approval of the Arab Ministers of Interior Council of the Arab Security Strategy, January 7 of 1983, followed by the adoption of the Arab Counterterrorism Strategy in 1997, which included elements aimed at coordinating counterterrorism efforts in the Arab countries, and strengthening cooperation with the international community. This strategy is based on a set of components, whether on the level of national counterterrorism policies or at the level of Arab counterterrorism cooperation.

The third situation in the Arab League counterterrorism efforts is the Arab Counterterrorism Agreement, which was concluded by the Council of Arab Ministers of Interior and the Council of Arab Justice Ministers, April 22 of 1998; it is the main legal counterterrorism pillar in the Arab League. Then the Arab Strategy for ideological Security came into play, which was issued by the Council of the Arab Ministers of Interior in its thirtieth session, held in Riyadh, March 13 of 2013. It has been the fourth milestone, aiming at confronting the ideologies drummed up for by deviant ideological trends and confronting the disinformation campaigns, while disseminating ill-intentioned ideas that push those deceived into joining extremist organizations.

### Analyses and Studies

As revealed by the analyses of the current issue of At-Tahalof Magazine, Lasina Diarra from Côte d'Ivoire addressed the relationship between ISIS and Al-Qaeda in the Sahel, criticizing some analyses that stated that the clashes between the two organizations in the early 2020s in the Sahel are likely to exhaust the forces of terrorist movements as a whole, confirming that such analyses misunderstand the essence and purpose of terrorism, especially in the Sahel, because ISIS in the Greater Sahara (ISGS) is nothing but a corridor for Al-Qaeda; between these two terrorist entities, there are bridges of solidarity.

Hamdi Bashir discussed the economy and important sources of funding of terrorist organizations in West Africa, addressing the challenges of combating terrorist financing, such as political corruption, intelligence corruption and poor rule of

law. He called on the international community to strengthen cooperation with West African countries in all areas, especially sharing intelligence information to further help target individuals and entities involved in activities supporting terrorist organizations across the region.

In the Research Studies Section, Sylvie Taussig, French researcher addresses the Third Approach Theory, being an alternative world to the far-right, whose roots are deeply ingrained in and go back to the end of World War II, and which fed an empowered feeling of the supremacism of the white man or European civilization.

### Issues Section

In the "Issues" Section, Abdul-Aziz Agraz, senior researcher, discussed the Dark Web and Terrorism, explaining the terrorist activity in various websites since the late 1990s, which created new counterterrorism blocs via cyberspace, especially after terrorists resorted to covert communication, using the Dark Web.

Dr. Haoues Seniguer provided an analysis of the French youth and extremism, turning the spotlight on the challenges surrounding the terms "youth" and "extremism." The use of the term "youth" per se in discourse may cause this group to be viewed as a social unit, and an organized group with common interests, and limiting these interests to a biologically determined age; this is clearly defined futility because by categorically misusing language under the same concept, we include social worlds that have almost nothing in common.

We face the same challenges when it comes to the term "extremism," which we must look at just as we look at the term "youth." Extremism has different connotations, as well.

Seniguer indicated that the relationship between extremism and youth does not concern segments of the French Muslim population only, and the ideology of exaggeration or extremist ideology cannot be reduced to its religious and terrorist side only. Therefore, it is erroneous to describe a violent extremist as necessarily coming from militant circles in French Islam because this contradicts reality and truth.

By the same token, the claim that such an extremist is a central or fundamental phenomenon of Islam in France is also spurious. This is true because such extremism is feeding on the sidelines of the phenomena that represent French Islam.

### ISIS in East and Central Africa

In the Focus Section, Ahmed Askar, senior researcher, addressed the spread of ISIS in East and Central Africa. Both Mozambique and the Democratic Republic of the Congo have become a new center for ISIS in the Great Lakes region, which has been called ISIS of Central Africa, in addition to the expansion in East Africa, specifically Somalia to tighten control over th territory far from its traditional rules and to wield influence on the continent. The United Nations estimates the spread of two thousand ISIS militants in the Democratic Republic of the Congo, Mozambique and other countries in East Africa.

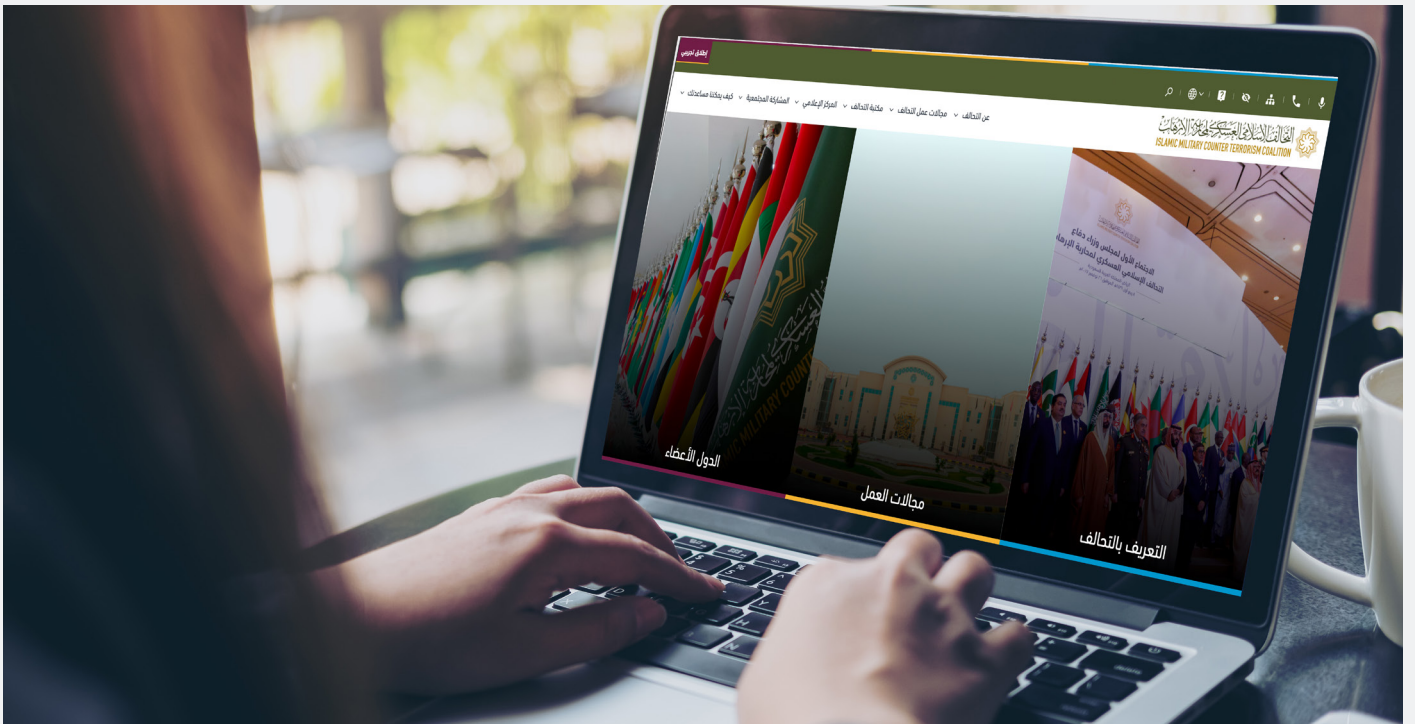
The researcher also spelled out that the spread of ISIS in East and Central Africa increases international and regional fears that the region will become a regional center for terrorism and a platform for expansion to other neighboring regions, which augurs ill for a second wave of ISIS across Africa. 🌸

## AL-QURASHI ASSIGNED ASSISTANT TO MILITARY COMMANDER



**Major-General**, Abdullah Hamid Al-Qurashi, assumed his duties as assistant to the IMCTC military commander. On this occasion IMCTC held a reception for Major-General Al-Qurashi, April 11, 2021. 🌸

## NEW WEBSITE OF IMCTC LAUNCHED



**Under** the auspices of Major General, Mohammed Saeed Al-Moghedi, Secretary-General of IMCTC, the new website of IMCTC was launched at the beginning of the month of Ramadan 1442 (April 13, 2021) to be a platform for introducing IMCTC domains, objectives, achievements, news and activities in three languages: Arabic, English and French. The IMCTC publications (At-Tahalof Magazine), (Allied Bulletin), (Book Review) and (International Reports) will be made accessibly available. 🌸