MARCH EDITION 2021, NO. 25

متحالفون

ALLIED: MONTHLY BULLETIN ISSUED BY IMCTC

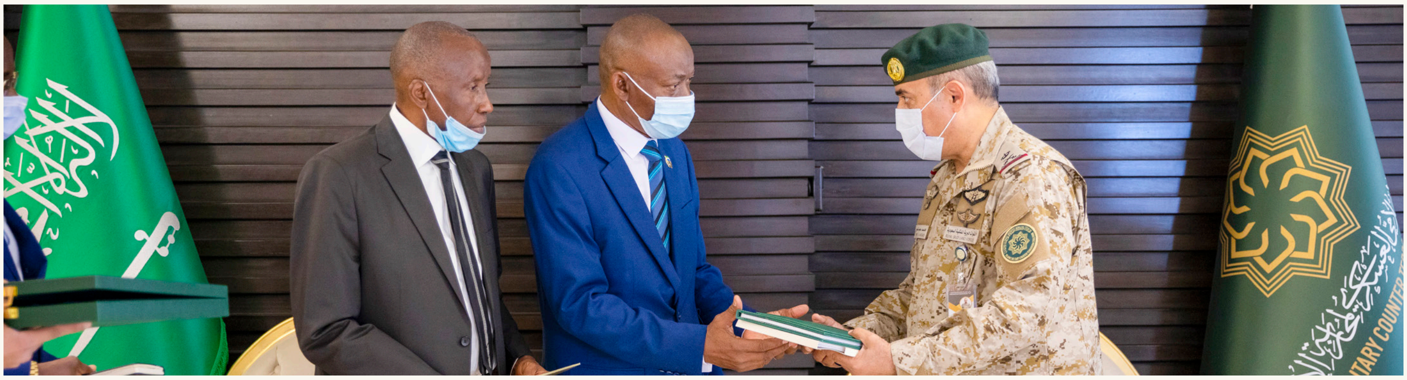
MEMORANDUM OF COOPERATION BETWEEN IMCTC AND AL-IMAM UNIVERSITY

Maj. Gen. Mohammad Saeed Al Moghedi, IMCTC Secretary-General, and H.E. Prof. Ahmed Salem Al Ameri, President of Al-Imam University in Riyadh, signed a memorandum of cooperation, on February 28, 2021.

Al-Moghedi emphasized that the said memorandum will strengthen the partnership between the two parties, as a manifestation of their leading local, regional and international role in combating extremism and terrorism, looking forward to making use of such cooperation through visits, sharing information, publications and training efforts.

H.E. Prof. Al-Ameri commended the IMCTC counterterrorism efforts, hoping that this partnership would contribute to achieving the goals of the two parties across the Arab and Muslim communities.

IMCTC SECRETARY-GENERAL RECEIVES THE ACTING CHARGÉ D'AFFAIRS A.I. OF THE REPUBLIC OF SIERRA LEONE



The IMCTC Secretary-General, Maj. Gen. Mohammed bin Saeed Al-Moghedi, received on Thursday, February 11, 2020, Mr. Hassan Koroma, the acting chargé d'affairs a.i. of the Republic of Sierra Leone to the Kingdom of Saudi Arabia, and the accompanying delegation. The two sides explored venues of cooperation and common visions in the field of counter terrorism. During the visit, the Ambassador was provided with an overview of the IMCTC's efforts in the four domains of action: ideology, communications, counter-terrorist financing, and military, as well as its role in coordinating and intensifying member countries' efforts in this regard. He met with the delegates of the Republic of Sierra Leone to IMCTC and got a brief about their work across the domains of counter-terrorism. The Ambassador also commended the positive role that IMCTC plays in establishing strategic partnerships among member countries, supporting states, and international organizations, in addition to strengthening relations and continued cooperation with all nations of the world to enhance capacities and share global best practices, information, and expertise in counterterrorism, and to join other international efforts to maintain international peace and security.

TERRORISM BETWEEN THOUGHT AND BELIEF

IMCTC held a presentation entitled "Terrorism between Thought and Belief", on Monday, 1 February 2021, at its headquarters in Riyadh. The presentation was delivered by Dr. Zayed Al-Harthi, Delegate of the Kingdom of Saudi Arabia to IMCTC. At the beginning, Al-Harithi emphasized that the phenomenon of terrorism has subsided, but humanity needs some time to be able to get rid of its negative and destructive consequences. One of the reasons behind the lack of control over the phenomenon of terrorism is that the basic and conceptual gateway to this phenomenon is perplexed. One of the most important gateways that contribute to developing plans and programs to combat this phenomenon is to define the key terms because of the controversies that have surrounded them so that they become a basis and a point of departure for the upcoming protective and strategic programs.

Al-Harthi talked about the overlap between the terms of ideological deviation, ideological extremism, ideological terrorism, ideological exaggeration ... among others. Over decades, linguists, psychologists, sociologists and specialists in religion and security have dealt with these terms in detail. Among these concepts, only the definition of terrorism and extremism was globally controversial. The term of terrorism is defined according to the background, beliefs, interpretations and goals of the one who defines it.

Al-Harthi added that it is important to differentiate between such terms in order to accurately build up new concepts that help develop a successful strategy to address this challenging international phenomenon. He added that the best definition of extremism is: "A relative term used to describe ideas or actions that are ideologically unjustifiable, and that the terms of extremist and extremism are almost used by other parties, so there is no religious or political sect or party that calls itself extremist." Thus, the concept of extremism is difficult to define because it overlapped with other concepts such as exaggeration and deviation. They are ideological concepts like those of personal and abstract concepts such as intelligence, introversion, depression and others. They are distributed among human beings as illustrated by the figure (1):

Al-Harthi concluded that the common definition of extremism is that it is a violation of society values, norms, ideologies and behavioral style. It is also expressed by isolation, withdrawal and negativity, or the adoption of different values and standards. The defense of such concepts may lead individuals or groups to violence, aiming to bring about change in society and impose opinion by force. This is related to terms including dogmatism and intolerance, i.e. intellectual stagnation, converting ideas into beliefs, and closed-mindedness. Those who adopt this behavior are unable to accept any ideas that differ from what the they believe in.

Measuring and judging extremism and terrorism

Dr. Al-Harthi explained that the main problem does not lie in terrorist acts and violent extremism, as they are evident and visible; they are countered by the security and judicial authorities. However, the world nowadays is facing difficulties in answering important questions such as: Since (ideological extremism) and (ideological terrorism) are theoretical terms that are related to actions, victims and traumatic events, how can they be measured? Is it necessary for someone who is ideologically extremist to be a terrorist? Al-Harthi stressed the importance of differentiating between ideological extremism and physical aggression, and that

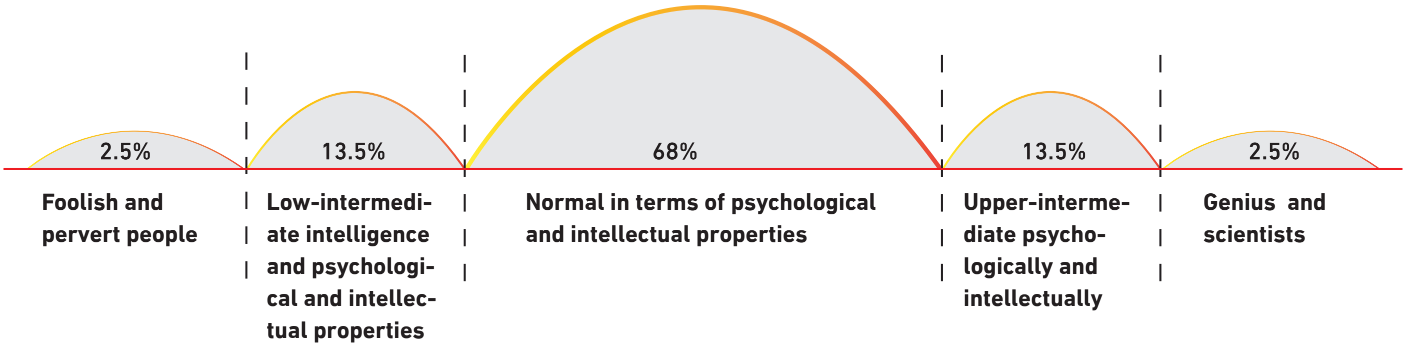


FIGURE (1): INTERRELATED CONCEPTS OF EXTREMISM

it is important scientifically speaking to understand ideological extremism and terrorism separate from terrorist acts. There should be scientific and objective measurements of ideological extremism that serve as a reference for countries, organizations and interested individuals. These terms should be judged like any other conceptual terms, be them personal such as mental illnesses and various personality traits, or social characteristics. Since research centers and universities have produced many standards for such terms, the need to know the metrics that measure the terms of ideological extremism and terrorism are still there and of utmost importance.

Al-Harthi pointed out that the American Psychologist journal addressed this problem (2017) in a special issue entitled (The Psychology of Terror) which dealt with the following topics of discussion: How do individuals become extremists? How to predict who among extremists will become a terrorist? How does the shift from nonviolence to violent extremism and then to terrorism happen? Researchers Clark McCall and Sophia Moskalenko, in a paper entitled "Understanding Political Extremism: The Hierarchical Model," proposed the dual hierarchical model to differentiate between extremism in opinion and extremism in action. After that, Clark McCall developed the model in a study published in the Journal of Terrorism and Political Violence (May 2020). The model emphasizes the importance of differentiating between these two types of extremism. Mixing between them will lead to difficulties in addressing the issue, and to an increase in violence and terrorism, because in this case, the measures to counter them would harm individuals or groups only for their believing in a specific ideology or belief.

Al-Harthi stressed that we need to set up universal and objective measures to address ideological extremism and terrorism. These measures should be away from subjectivity and should not be related to different political and religious backgrounds. They should also have scientific and field references of experts and specialists.

Thought, Belief and Terrorism

In his presentation, Dr. Al-Harthi analyzed the terms of Thought, Belief and Terrorism. As for Thought, he said that it is the opinions and ideas that result from a regular thinking process; however, a thought that is not organized and coherent cannot be called thought. That is why the concept of thought is interrelated with organization, coherence, inference and cogency. As for Belief, it is what the heart believes in firmly, be it religious or something else. The difference between Belief and Thought is that the former is characterized by firmness and stability, while the latter is flexible and relatively stable; the thinker can modify his thoughts, but cannot modify his belief whatsoever. Al-Harthi added that it is essential to differentiate between Thought and Belief for setting up plans, programs and strategies to counter the changes of terrorism, and protect individuals and societies from its dramatic effects.

Complex motivations

Al-Harithi explained that the motivations of terrorist acts are very complex to the extent that even those who carry out the terrorist acts may not know exactly why they do that. He cited what John Horgan, who is one of the most important global references in terrorism studies, concluded after interviewing dozens of former terrorists. He said that when asking terrorists about their motivations for carrying out their acts, the shocking answer is often: (I don't really know). This means that many of those who joined the struggle in Syria and Iraq have no idea about the sectarian conflict that they engage themselves in.

Conclusions

At the end of the presentation, Dr. Al-Harthi presented a number of important conclusions, including:

- ▶ Terrorism is a complicated phenomenon, so it cannot be countered or prevented from one side, approach or theory.
- ▶ There is a contradiction between the main concepts of the discussed phenomenon, which are extremism, ideological extremism and deviation, and ideological and physical terrorism.
- ▶ In order to avoid dwelling into the details of the phenomenon without establishing ideas correctly, it is important to identify the best terminology of terrorism, and develop the objective scientific standards of the concepts of extremism and ideological terrorism prior to planning to counter them. A very essential step is to differentiate between thought and belief.
- ▶ Taking advantage of all specializations and international efforts that work on a comprehensive and universal approach to the phenomenon, apart from exclusivity and fanaticism for local or regional directives and backgrounds.

Information and Communication Technology Spreads and Counters Extremism and Terrorism at the Same Time

In the age of communication technology revolution, the ability of terrorists to plan, implement, finance and recruit has doubled. If the terrorists of the last century were alive, they would envy the terrorists of the twenty-first century because today terrorists are able to spread their poisonous thoughts and propaganda to millions of people with one click, and in the same way they are able to transfer money and buy weapons. At the same time, these technologies have strengthened the capabilities of states, governments and peoples to fight terrorism. So, they are used by terrorists and those fighting them. This made communication and information technology the topic of the symposium of the Islamic Military Counter Terrorism Coalition (IMCTC), which was held at its headquarters in Riyadh, on the third Wednesday of February 2021, entitled "The Role of Information and Communication Technology in Spreading Extremism and Terrorism and Counter Measures". The symposium was moderated by Brig. Gen. Dr. Mustafa Ibrahim Suwaisi, Delegate of Libya to IMCTC, and the presentation was delivered by Brig. Gen. Rashid bin Mohammed Al-Dhaheri, Delegate of the United Arab Emirates to IMCTC, and Brig. Gen. Tawfeeq Mufleh Al-Bataineh, Delegate of the Hashemite Kingdom of Jordan to IMCTC.

The symposium covered two topics. The first one addressed the relationship between information and communication technology, on one hand, and terrorist organizations, on the other hand. The second topic addressed the measures to countering extremism and terrorism using information and communication technology.

The first topic included an explanation of the use of computer by terrorists and their threats to disable computers and networks with all information they contain in order to terrify governments and people and force them to meet social and political demands. The symposium provided a definition of online extremism which is "Harnessing the Internet and all related electronic services for setting up websites, and using sending and receiving services that facilitate the transmission of extremist ideologies and violence, whoever the party that adopts it."

The most important motivations of using the Internet by terrorist organizations are its features and capacity in terms of speed, impact, effectiveness, low cost, ease of use and being not well-controlled and monitored.

These facts make the Internet a platform used by terrorist organizations to spread their propaganda, prepare for operations, and recruit new individuals. They are especially interested in social media that have many features including:

- Creative artistic form.
- Services that bypass website blocking.
- Continuous update of content.
- Coordination among sites.
- Availability of audio and visual materials.
- Additional options.

Millions of messages, websites and tweets

The symposium provided some statistics of online violence and extremism. There are 270,000 extremist websites, 16 terrorist multilingual media networks and 9 million clips in English on YouTube, more than 47 thousand in French, more than 20 thousand in Russian, and more than 12 thousand in Arabic. 70% of terrorists' supporters spend a long time on Twitter, posting 2,612 tweets per hour. 93% of which are text tweets. Some of those tweeters update their account every 5 minutes.

The first topic of the symposium also included an explanation of Twitter's role in spreading ISIS terrorist ideology. Through Twitter, ISIS tried to prove the existence of its alleged state, support lone wolves, spread fear and recruit supporters, promote its ideologies about success on the battlefield, and improve the image of suicide bombers by publishing positive pictures of them after their deaths. ISIS also used Twitter to identify its sympathizers by monitoring their comments and sending them private messages to persuade them to join it, carry out a terrorist act, or assist in a terrorist act in their countries.

Countering methods

As for the second topic, it dealt with countering cyber terrorism and the most appropriate measures to counter it, including: blocking websites, legislating laws and establishing penalties, establishing departments of security to counter "cyber terrorism", and improving government capabilities to counter cyber threats.

The second topic also included an explanation of the UN role in countering online extremism and terrorism. The UN issued several resolutions through its General Assembly that revealed the increasing global awareness of the non-peaceful use of communication and information technology. In response to the technical progress and the increase of terrorist electronic operations, the UN worked on three procedures: warning and raising awareness, issuing resolutions, and developing strategies to counter terrorist activities.

The UN issued the Global Counter-Terrorism Strategy in 2006, which called for the use of the Internet as a tool to counter the spread of terrorism. It also called for coordination of efforts at international and regional levels to counter online terrorism in all its forms.

The Security Council issued Resolutions No. 1373 of 2001 and No. 1566 of 2004, which obligate member states to take legislative and non-legislative measures to counter terrorism, and to implement international conventions and protocols related to terrorism. It also issued Resolutions: 1624 of 2005 and 1963 of 2010, which include condemning online terrorist activities, and calling on member states to work together to prevent terrorists from exploiting the Internet technology.

International cooperation in countering cyber terrorism

In addition to the two topics, the symposium reviewed international plans to counter cyber terrorism. The UN has been moving forward in countering online terrorism and extremism. It has moved from condemnation and warning level into issuing resolutions for countering this type of terrorism and developing comprehensive and effective plans and strategies. The international efforts, foremost of which are the United States efforts, provided a good development in confronting the threat of online terrorism and extremism. Several means and methods including legislative, technical, military or security ones, were an outcome of international cooperation and coordination to counter this phenomenon.

Also, the European Group took some steps aiming to develop the information network and secure it from being hacked by terrorists. It issued new legislations to early detect such acts and prosecute their perpetrators.

The Saudi capital, Riyadh, hosted the International Conference on Combating Terrorism in 2005, which issued recommendations regarding cooperating and coordinating among countries on the highest levels, establishing a joint international body in coordination with the UN to exchange information and experiences, and developing methods, trainings, legislations, technologies, and activities that strengthen national capabilities to counter terrorism.

Arab efforts

The symposium showcased Arab efforts to counter online terrorism and extremism, including the Arab Counter Extremism and Terrorism Strategy, the Arab Convention for the Suppression of Terrorism in 1998 and the Arab Convention in Combating Information Technology Offences. Moreover, the recommendations of the Eighteenth Council of Arab Ministers of the Interior in 2015 called for taking the necessary measures to curb the "spread of extremist and sectarian discourse, and counter terrorism."

On the national level, the symposium showcased the efforts of the Kingdom of Saudi Arabia and the United Arab Emirates in countering cyberterrorism and extremism. Saudi Arabia developed The Strategy to Confront Ideological Deviations in the Saudi Society in 2007, and developed comprehensive plans to detect suspicions on the Internet and social media. It also issued The Cybercrime Law in 2007, and established the Etidal Center in 2017.

The UAE established the centers of Hedaya (2012) and Sawab (2015), and developed The International Initiative for the Criminalization of Cyberterrorism in 2017, and several laws, including:

- "International Judicial Cooperation in Criminal Matters" in 2006
- "The Law on Combating Terrorism Offences" in 2014.
- Federal Decree on Anti-Money Laundering and Countering the Financing of Terrorism
- Federal Law No. 5 of 2012 on Combatting Cybercrimes and its amendments in 2016 and 2018

Summary and recommendations

The symposium concluded that cyberterrorism and constant scientific progress are interrelated. It is difficult to find absolutely reliable methods to protect the information system from being hacked although most countries and institutions are adopting cyber-security measures to protect their information systems from being hacked by terrorist attacks.

The symposium made a number of recommendations including:

- Spreading the culture of prevention and educating society about the dangers of terrorism in general, and cyberterrorism in particular.
- Follow up on the enactment and development of laws and legislation in order to bridge the gaps related to cyberterrorism in the age of rapid technological development.
- Creating an international legal system under the umbrella of the Islamic World to coordinate the states' efforts to combat cyberterrorism, taking into account the UN laws and legislations in force.
- Constant readiness for any cyberterrorism operation, and development of perceptions of potential risks and control methods.
- Securing information networks, communication systems and energy sources on the material (building durability, security measures, security escorts) and technical (training, protection programs) levels.
- Supporting scientific research related to information security and countering cyberterrorism, and developing national protection programs in order to dispense with importing protection and encryption programs.
- Qualifying security personnel on cyberterrorism and methods of monitoring and investigation.
- Member states of Islamic countries that are advanced on the material and technical levels should help developing states to be able to develop their technical capabilities to counter terrorism.

TRAINING COURSE ON COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

IMCTC in cooperation with the Financial Academy held two training courses themed Combating Money Laundering And Financing Terrorism provided by Hassan Khalaf Al-Faouri, senior trainer. The trainees were of two groups and two different time slots: January 25 and 26 and February 14 and 15 of, 2021 respectively. The said training course aimed at raising the target trainees' awareness and education, enabling them to understand anti-money laundering and counter-terrorist financing operations, in such a manner as to be well-equipped with the ability to put them in place. It also provides them with the skills to detect financial crimes.

MONEY LAUNDERING CRIME

The trainer spelled out that the purpose of money laundering is to conceal the true source of the funds funneled by illegal means, legitimize them, use them in the economic cycle and transfer them across international borders in the channels of legitimate financial institutions. Therefore, the relationship between money laundering and corruption is glaringly obvious; the systems that lack transparency and oversight have high levels of money laundering and corruption, according to Transparency International's Global Corruption Report.

The trainer revealed that money laundering operations have become a global risk. The percentage of money laundered was estimated between 2% and 5% of global GDP, i.e., between $ 800 billion and $ 2 trillion annually, which can be notoriously manifested through the following:

- ▶ Drug trafficking
- ▶ Arms smuggling and trafficking
- ▶ Smuggling of goods and products across borders
- ▶ Prostitution and sex trade
- ▶ Bribery and administrative corruption activities and profiteering from public office
- ▶ Income resulting from thefts or embezzlement of public or private funds
- ▶ Crimes of forgery and counterfeit
- ▶ Fraud and deception
- ▶ Tax evasion
- ▶ Human trafficking
- ▶ Crimes of extortion and kidnapping for money

CRIME ELEMENTS AND EFFECTS

The trainer mapped out the elements of money laundering crime into two types: the first type is material, which includes the location of the crime (funds, proceeds, and revenues), and the behavior (possession, acquisition, use, transfer, and concealment); the second type is moral, which includes "criminal intent", meaning the direction of the perpetrator's will to commit the criminal act.

Then the trainer reviewed the basic stages of money laundering operations; it begins with the stage of deposit or replacement, which means to introduce funds resulting from illegal activities into the banking financial system (banks). The second stage is camouflage, concealment or coverage, by transferring such funds to conceal the illicit origin, such as transfers to other banks, purchase and sale of investments and insurance contracts). The next stage is merger, by entering the funds again into the financial system by purchasing assets, stocks, real estate, or valuable commodities or investing them in projects. The money laundering process may not go through the previous stages (deposit, concealment, merging) and take place in one or two stages.

The trainer also analyzed the negative effects of money laundering operations. Economically, they weaken the state's ability to well implement economic policies efficiently, weaken economic growth, disrupt the foreign exchange market, bring about loss of confidence in banks, collapse of stock exchanges and financial markets, rise in prices and increased levels of inflation. Politically, it causes infamy and notoriety, such as the spread of political and administrative corruption and abuse of influence, damage to the reputation of the state and the increase in the influence of money launderers in the state and their influence on legislation and laws. Socially, money laundering operations exacerbate unemployment, ubiquity of job, corruption, malfeasance and venality.

INTERNATIONAL INITIATIVES

The trainer highlighted and discussed international initiatives in combating money laundering and terrorist financing, showcased and spearheaded by the Financial Action Task Force (FATF), established in 1989 by the Group of Seven Industrial Countries, and now includes 37 countries (members), and two regional organizations, namely the European Commission and the Cooperation Council for the Arab Gulf States. The FATF issued 40 minimum standards for combating money laundering and terrorist financing recommendations, which have been adopted by more than 180 countries. In June of 2019, the Kingdom of Saudi Arabia became the first Arab country to have joined the FATF.

The Basel Committee issued a document of principles on preventing the use of the banking system for the purposes of money laundering crimes in 1988.

TERRORIST FINANCING

Terrorist financing means the operations of collecting funds to be used in whole or in part in the implementation of actions intended to cause the death or serious injury of a person, or the purpose of which is to terrorize a target population, or to force a government or international organization to do or abstain from any action.

The trainer believes that terrorist financing is a type of money laundering, but it is different in that such funds may start out clear; the source of the funds may be legitimate.

The amounts of terrorist financing are usually small, arousing no suspicion, and are not intended to gain wealth. Such funds may be transferred through the banking system using the method of remittances or by trafficking money across borders.

PATTERNS OF MONEY LAUNDERING AND TERRORIST FINANCING

The trainer listed some patterns related to money laundering and terrorist financing, including:

- **Transfer:** Any alternative transfer services, such as hawala, securities, which are informal means of transfer, based on trust networks, and often work parallel to the traditional banking sector, but they are not organized.
- **Organization:** It includes various operations (deposits, withdrawals, and transfers), often involving a group of people, and a large number of small-value transactions, and sometimes various accounts to avoid obligations of financial institutions to report suspicious financial transactions.
- **Currency Exchange:** It helps to traffic money across countries, or take advantage of poor reporting obligations of currency exchange institutions, such as buying traveler checks.
- **Trafficking Currency:** It is a secret movement of currency across borders to avoid cash disclosure procedures.
- **Credit Cards and Checks:** It is used to access money deposited in bank accounts, often in another country.
- **Asset Purchases:** The proceeds of criminal activities are invested in expensive goods, such as real estate, cars and stocks to take advantage of less reporting requirements.
- **Using Telegraphic Transfers:** transferring funds electronically between banks, often to another country.
- **Commercial Money Laundering:** It usually includes mis-invoicing, and the use of commercial finance and goods to avoid financial transparency.
- **Investing in Money Markets:** concealing the source of the proceeds of criminal activities by purchasing negotiable securities.
- **Business Investment:** it is a major step in money laundering, which includes combining the proceeds of criminal activities with legitimate business funds.
- **Using Shell Corporations and Companies:** Concealing the identity of the people who control the funds.
- **Using Intermediaries and Trustees:** Using a third party to conceal the identity of the people who control illicit money.
- **Using Professional Service Providers:** Such as lawyers, accountants, and brokers to conceal the identities of the beneficiaries.

SUSPICION INDICATORS

The trainer provided indicators for money laundering and terrorist financing:

- **Client-Based Indicators:** a given suspect provides fake or suspicious data, or data that is difficult to verify or the amount of the operation is not proportionate to the nature of work.
- **Account-Based Indicators:** making frequent and many large transfers, incoming transfers to the account, followed by withdrawals or transfers, or the value or type of transactions not commensurate with the nature of the account, or sudden activity on an inactive account, especially with a high value.
- **Indicators of Financial Transactions:** buying or selling securities in abnormal circumstances, or paying customers loans against assets of unknown sources.
- **Indicators of suspect behavior:** being careful not to deal directly with bank employees, preferring to deal with automatic teller machines, with multiple bank accounts, and the suspect's request to cancel the transaction once the bank's employees request important information.

The key suspicion indicators of terrorist financing include:

- Transferring from or to countries experiencing political or security turmoil.
- The value of the transactions is not proportional to the information about the suspect, activities, income, lifestyle and behavior.
- Communicating with persons or entities not directly related to the suspect.
- Communicating with many people of different nationalities.
- Possessing a large amount of cash across borders.
- Transferring to several persons in different countries without an apparent reason.
- Inclusion of the name of the suspect or the real beneficiary on the United Nations lists.

SECURITY OF MOBILE SMART PHONES

IMCTC held a presentation entitled "Security of Mobile Smart Phones" on Tuesday, 23 February 2021, at its headquarters in Riyadh. The presentation was delivered by Dr. Ihab Al-Rasn, an assistant professor of Internet technologies and distributed systems at King Saud University. At the beginning, the presenter noted the importance of mobile phone security, especially smart phones which are portable computers that allow their users to get access to the Internet and download apps and games easily. Smart phones also allow users to store their personal information. We have to protect our data stored on smart phones because, just like the data on PCs and laptops, they are vulnerable to hacking or espionage, or to be lost or stolen.

Cyberattacks

According to Kaspersky Lap's statistics, the number of cyberattacks in the Middle East, Turkey and Africa (META) is 1.5 million attacks a day, and 575 million in a year. The Kingdom of Saudi Arabia has experienced a remarkable increase in this type of attack, with 387% of ransomware attacks, 11% of malware infections, 43% of Trojan horse attacks, and 4% of malware attacks.

An analytical study conducted by the same company revealed that in the second quarter of 2019, the violent phishing attacks amounted to more than (973,000) attacks in the Kingdom of Saudi Arabia, (617,347) in the UAE, (492,532) in Egypt, (193,379) in The Sultanate of Oman, (128,356) in Qatar, (106,245) in Kuwait, and (67,581) in the Kingdom of Bahrain.

Phishing attack is one of the oldest and most flexible types of cyberattacks and social engineering. It has several ways of capturing users, and it has different purposes.

The wide reach of mobile phones and other smart devices has led to an increase in interest of cybercrimes and hacking. The cybercriminals try to access to sensitive data, download malware and commit phishing. In the first half of 2019, a hundred million attacks on smart devices were detected worldwide. Electronic piracy statistics of 2019 show that more than 24,000 malicious smartphone apps were blocked from app stores every day. A study by Veracode for Security Tests revealed that about 59% of organizations have been affected by the increase of malware because of unsafe mobile phones that contain insecure apps.

Root and Jailbreak

The use of "root" tools on Android devices, and "jailbreak" on Apple devices is one of the most common methods of attacks on smart phones. When an Android device is rooted, every one may become a super user and do many features like installing themes, improving system performance, and increasing battery life. However, "root" tools work behind user's back and may easily access to user's data and download some malicious programs.

As for "jailbreak", it is a process on "IOS" system of Apple phones which bypasses the firewall of installing spyware on iPhone and iPad devices. The hacker or spy needs to do a "jailbreak" for the user's device to be able to bypass the restrictions of Apple on iPhone and iPad devices, and install untrusted apps. Therefore, the user should make sure that his device is healthy and not jailbroken. In addition, the user should keep his device up to date and use apps such as SnapStats that provides details about iPhone devices to know whether they contain a "jailbreak" of not.

As for VPN, it provides an encrypted tunnel online in which the user's device is connected to a server of one of the tunnels' networks. It is called a tunnel because, unlike other encrypted browsing traffic like the "https" protocol, it hides all services, protocols and contents. Because your browsing traffic passes through a VPN server, it needs access to the intermediary server to analyze user activity. It is important to choose carefully the suitable VPNs and to use many of them; This distribution of data traffic limits the impact of hacking on the device.

Social engineering

The presenter talked about social engineering in smartphones. He said that it is a method of collecting data socially, like talking

to employees of a facility. The process of social engineering may occur through a phone call or an e-mail, or by notifying the target with a message. When he clicks on the link found in the message, the entire mobile phone is hacked, and the hacker professionally accesses the victim's data, and bank accounts.

The presenter gave a number of recommendations that help to protect against social engineering, such as establishing strict security policies, and educating employees on such types of fraud.

Targeting eminent personalities

In a Bitcoin-related fraud, Twitter accounts of eminent persons have been hacked. They include the accounts of Elon Musk, Jeff Bezos, Bill Gates, Barack Obama, Joe Biden and Kanye West, among others. "Everyone is asking me to return the favor, send me 1000 dollars, and I will send you 2000 dollars" This is a tweet on Bill Gates' account. Twitter said that parties that know "details of internal systems and tools of the company" launched a "coordinated" attack targeting the company's employees. They used the details to control prominent and trusted accounts, and send tweets with their names. In addition, the Cloud service was hacked and celebrity photos were stolen. These operations happened because of viruses on customers' computers, or because of their downloading of a malicious apps on their Android devices.

Hacking bank accounts

Some fraud actions have been committed to a number of Al-Mubasher retail customers in a bank. Please be careful of pop-up messages that ask you to enter a mobile number, mobile model, ATM card number or PIN. Remember that the apps of Al Mubasher Individual Service do not ask you to enter such information.

Be careful of apps called "Al Rajhi mToken", "mToken" and "Alrajhicertificate." They are fake apps that steal the information and passwords of the messages sent by the bank to access to Al Mubasher Personal Service.

Safe usage

Social media can be offensive and harmful if they are used to spread lies, hate, and rumors, or when they are used to attack people, violate privacy, re-post offensive clips, do identity fraud, among others.

How to know whether your phone is hacked or not?

The presenter explained that the most effective hacking methods are malicious apps because they work in background without being detected or noticed in the list of running apps. Malware may use smart phones as a tool for advertising, and consume a large portion of the device's charge. The following are signs that appear on a hacked device:

- Slow performance.
- Sudden slow response
- Apps running in the background after being closed.
- E-mails or SMSs in the sent folder and not sent by you.
- The interface of your phone changes by itself.

Protect your smartphone

At the end of the presentation, the presenter provided tips for protecting smartphones. The most important of which are:

- Set up passwords on your phone.
- Ensure the validity of the apps you want to download on your phone.
- Activate the two-factor authentication feature.
- Read the instructions and privacy policy before downloading apps that may access to your personal data.
- Use biometric features such as fingerprint and face recognition.
- Avoid downloading software from unknown sources.
- Keep your operating system up to date, including the installed software and the security software that save your device.
- Backup your data to avoid any loss, theft, or encrypting ransomware.
- Install anti-virus software to protect your phone.
- Activate the remote data wipe feature in case of a theft or loss.
- Scan the apps installed on your phone to ensure that there is no malicious software that installed without your knowledge.
- Do not share passwords or PIN with anyone, even your nearest.
- When using a home or external wireless network, make sure that it is encrypted and trusted.

IMCTC MAGAZINE COMES OUT AFRESH

SIXTH EDITION RICHLY CREATED AND BEAUTIFULLY DESIGNED

The sixth edition of the IMCTC Magazine was published in February of 2021 in three languages Arabic, English and French. This edition featured new look and distinct visual identity to better provide the reader with a rich knowledge that brings together the strength of content and the quality of innovative design, while enhancing the progress and continuous improvement of the IMCTC Magazine, both in the carefully diverse materials and the depth of content as well as renewed visual identity along with immaculate refinement of the output. The tremendous success materialized, thankfully, is due to the IMCTC concerted and unremitting efforts, spearheaded by the general superintendent of the IMCTC Magazine, Major General Mohammed Saeed Al-Moghedi, IMCTC Secretary-General.

It would be helpful to make a cursory glance at the new edition of the IMCTC Magazine, and walk the reader through the deeply approached themes through the various sections and subsections.

DIVERSE TOPICS AND GIFTED WRITERS

The sixth edition of the IMCTC Magazine came out with a special focus attached to creating wide-ranging topics, richly discussed by 18 eminent subject-matter writers of highly impressive expertise, coming from 14 countries of different continents. The writers are highly experienced and well-qualified in their respective fields, which well contributes to enriching the materials and providing an added knowledge value, and furnishing the readership with important scientific insights and ideas, in addition to the articles developed by the editorial team members on staff.

TOPICS

The themes selected for the sixth edition are covered in six chapters, arranged as follows:

OPINIONS: It approaches five articles: (1) How is thought formed and how is it radicalized? It is written by Prof. Zayed Al-Harithi, delegate of the Kingdom of Saudi Arabia to IMCTC in the Ideology Domain; (2) The Woman Victim and Rescue From the Clutches of Extremism and Terrorism by Bedai Sherif Mukhtar Ballari, researcher on extremism issues at the University of Diffa; (3) The Power of Ideas, Public Diplomacy and Terrorism by Dr. Al-Sadiq Al-Faqih, professor of political science at the University of Khartoum; (4) From The Social Motives to the Religious Cover: The Causes of Youth Radicalization in Niger by Dr. Umaru Makama Bawa, professor of political anthropology and researcher in contemporary Islam and the conflicts among communities; (5) Towards Preventive Reform Education in the Sahel Region by Mr. Seydou Khamma, inspector and researcher in education sciences in Senegal.

INTERNATIONAL INITIATIVES: Confronting Violent Extremism with Creative Multimedia by Dr. Dzynita Krabigovich, researcher in international relations and international and comparative political sociology.

INDICATORS: Terrorism through Global Index (GTI 2020): threats dissipating and challenges renewed.

ANALYSES: (1) The Impact of Violent Extremism in Mali and the Central Delta by Yida Seydou Diall, researcher on violent extremism issues in Central Sahel; (2) Changing Visions for Approaching Conflicts, the Mapuche People in Argentina as a Model by Dr. Mariano Gancido, professor of anthropology and conflict researcher.

FEATURE: (1) Terrorism as a Communicative Act: Terrorists Target the Public With Fear and Terror Before They Target Their Victims With Death and (2) Terrorist Media and Media Terrorism by Mr. Ashour Ibrahim Al-Juhani, Editor-in-Chief of the IMCTC

Magazine; (3) Semiotics of Violence: The Significance of Signs, Symbols and Images in Terrorist Media by Dr. Ammar Ali Hassan, novelist and researcher in political sociology; (4) Terminology of Terrorism in the Media Domain: Real Randomness and Necessity of One Unified Dictionary by Mr. Mohammed Saeed Al Futaisi, academic researcher in counterterrorism criminal policies from Oman; (5) Media and Counterterrorism: Responsibility and Impact by Dr. Howayda Mostafa, Dean of the Faculty of Mass Communication at Cairo University.

EXPERIENCES: The Cameroonian Counterterrorism Experience: From Confrontation and Containment to Integration and Rehabilitation by Prof. Othmanou Adama, researcher in ethnic and religious identities of the Chad Basin region.

REVIEWS: Sources for Achieving Balance in Intellectual Hypotheses by Prof. Mohammad Suleiman Al-Subaihi, Delegate of the Kingdom of Saudi Arabia to IMCTC in the Communications Domain.

RESEARCH STUDIES: IMCTC Tweets on Twitter: Studies and Analyses by Colonel Abdullah Mohammed Shadi, Delegate of the Republic of Yemen to IMCTC.

KEY ISSUES: International Migration and Global Terrorism by Dr. Idris Al-Kanbouri, researcher and writer and director of the Future Center for Research and Knowledge in Rabat.

IN THE SPOTLIGHT: Organization of Guardians of Religion by Dr. Mohammed Aref Al-Azamat, researcher in terrorism issues and former head of the Jordan Center for Extremism.

AUTHENTICITY: Recommendations from The Beacon of Islam, Religion of Justice, Tolerance and Moderation by Sharif Salim Alwan Al Husseini, Secretary General of Dar Al Fatwa, Islamic Supreme Council of Australia.

IMCTC NEWS: IMCTC started its scientific program for the new year with two keynote lectures in the ideology and communications domains: “Factors of Youth Joining Violent Extremism Organizations,” by Dr. Mansour Al-Qarni, Director of the Ideology Department at the IMCTC Center; and “Methods of Developing a Counter-Violent Discourse,” by Dr. Mohammed Sulaiman Al-Subaihi, Delegate of the Kingdom of Saudi Arabia to IMCTC in the Communications Domain.

WINDOWS: (1) Washington removes Sudan from the list of terrorism and classifies Saraya Al-Mukhtar as a terrorist organization; (2) International report warns of the repercussions of COVID-19 pandemic on counterterrorism efforts; (3) Europe supports counterterrorism measures; (4) Pakistan arrests the leader of an extremist group on a charge of financing terrorism; (5) fears of infiltration of the far-right into the army in Germany and the United States.

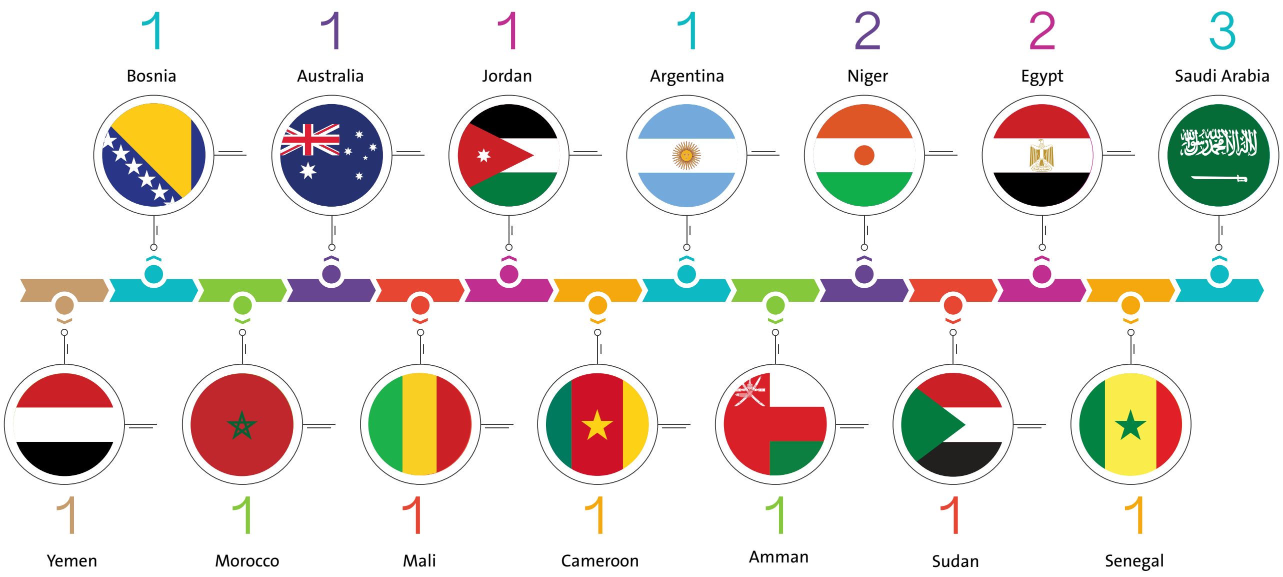
EDITORIAL: Towards A Code of Honor, In A Media-Based Follow-Up On Terrorism by the editor-in-chief.

Equally important, the policy used for the IMCTC Magazine put all the contributors’ articles into a rigorous editorial cycle. The written materials are published following meticulous evaluation, revision, review and linguistic and content-based correction; editorial oversight is closely exercised in terms of the validity and quality of ideas, the content and richness of the material, the high quality of the style and presentation, the accuracy of the meanings and the integrity of the language, and the precision of well-turned wording.

DESIGN, PRODUCTION AND PUBLICATION

Content, design and production are equally revamped and rejuvenated; the interior design and the presentations of the articles have undergone total improvement, providing a reader-friendly environment with careful content engineering, conflation and truncation where necessary. The 2021 editions of the IMCTC Magazine have adopted a new layout in terms of design and content, along with the elegant shapes, pie charts, bar graphs, images, tables and illustrations with new sections, such as windows and opinions. The carefully selected design shapes and layouts well reflect the richly discussed articles, featuring fitting titles with pinpoint accuracy and novelty, par excellence.

With the IMCTC Magazine superbly produced, the matching colors and the smartly attractive consistency make it a fabulously impeccable showpiece or chef d'oeuvre, visually and intellectually unputdownable, luring the readers into the pleasure of reading while feasting their eyes on the wealth of information brought at their fingertips most conveniently as hoped and desired.



Diverse Backgrounds and Nationalities of Authors Contributing to IMCTC Magazine, Issue 6

MARKING THE NATIONAL DAY OF THE REPUBLIC OF THE GAMBIA WITH MEMBER COUNTRIES

The Delegates of the Republic of The Gambia to IMCTC held a celebration to mark the National Day of The Gambia on 18 February 2021. The celebration was attended by Maj. Gen. Mohammed Saeed Al-Moghedi, IMCTC Secretary-General, General (retd) Raheel Sharif, IMCTC Military Commander, Delegates of the IMCTC member countries and some IMCTC personnel.

IMCTC MARKS THE INDEPENDENCE DAY OF THE STATE OF KUWAIT

The Delegate of the State of Kuwait to IMCTC held a ceremony on 25 February 2021 to mark the sixtieth anniversary of the State of Kuwait. The ceremony was attended by Maj. Gen. Mohammed Saeed Al-Moghedi, IMCTC Secretary-General, General (retd) Raheel Sharif, IMCTC Military Commander, Delegates of IMCTC member countries and some IMCTC personnel.

SECRETARY-GENERAL RECEIVES COMMAND AND STAFF COLLEGE DELEGATION

Maj. Gen. Mohammad Saeed Al-Moghedi received on 21 February 2021, a high-level delegation from the Command and Staff College of the Armed Forces, headed by Maj. Gen. Mohammad Jadooa Al-Ruwaili, College Commander and Director of the National Defense University.

The delegation was briefed on the IMCTC efforts and was provided with a detailed explanation by Maj. Gen. Al-Moghedi about the IMCTC initiatives and activities and the coordination of the counterterrorism efforts of the member countries across the four key domains of action: ideology, communications and counter-terrorist financing as well as the military domain.