JANUARY EDITION 2022, NO. 35

متحالفون

ALLIED: MONTHLY BULLETIN ISSUED BY IMCTC

ANNUAL PLAN LAUNCH 2022 OF IMCTC ACTIVITIES

IMCTC Secretary-General, Major-General Mohammed Saeed Al-Moghedi launched, December 29 of 2021, the annual program of the IMCTC activities 2022, in the presence of the IMCTC's Member Countries' delegates and personnel.

Al-Moghedi commended the achievements made in 2021, and expressed his appreciation to the great support provided by the headquarters country, and IMCTC Member Countries' delegates for their great engagement in the success of the 2021 plan, hoping that more achievements would continue to meet the aspirations of the IMCTC member countries and their respective leaders.

In a similar vein, Director of Ideology Department, Dr. Mansour Al-Qarni, reviewed the key features of the 2022 Plan, noting that it would be implemented in close coordination with the IMCTC Member Countries' delegates, in perfect harmony with the IMCTC strategy and associated initiatives, the IMCTC governance framework, and the IMCTC member countries policy in countering violent extremism and terrorism.

SECRETARY-GENERAL RECEIVES AMBASSADOR OF REPUBLIC OF CAMEROON

IMCTC Secretary-General, Major-General Mohammed Saeed Al-Moghedi, received at the IMCTC headquarters in Riyadh, December 8 of 2021, Ambassador of the Republic of Cameroon to the Kingdom of Saudi Arabia, Iya Tidjani along with the official delegation. Ambassador was briefed on the IMCTC counterterrorism efforts, the key role it plays in close coordination with the IMCTC member countries, and the Situation Room's monitoring terrorist acts.

For his part, Major-General Al-Moghedi called on the Republic of Cameroon to join IMCTC as a member country, given its political, economic and military position in the Central West African region, and its great counterterrorism experience. Al-Moghedi also commended its efforts in confronting Boko Haram and other terrorist groups that seek to wreak havoc, chaos, and destruction disguised in religion.

DIRECTOR OF ISLAMIC BROADCA TING UNION PAYS TRIBUTE TO IMCTC COUNTERTERRORISM EFFORTS

Director-General of Islamic Broadcasting Union (IBU), His Excellency Dr. Amr Mamdouh Al-Leithi, commended the IMCTC counterterrorism efforts and the pioneering role played by the Kingdom of Saudi Arabia in supporting IMCTC and nipping in the bud terrorism and criminal groups. The timely appreciation came in when Secretary-General received Director-General of IBU at the IMCTC headquarters in Riyadh, December 14, 2021.

TERRORIST PERSONALITY AND PSYCHOLOGY OF EXTREMISM

Psychoanalysis of terrorist personality has gained prominence across the global counterterrorism policies as it is seminal to dismantle terrorist ideology, rehabilitate and reintegrate terrorists into society and stave off involvement in terrorist organizations. Security and judicial treatment alone cannot pay off to eliminate terrorism. Terrorists remain a threat even after they are captured, imprisoned, and released. Many countries seek to develop various relevant programs, using different scientific methods. Perhaps the most important counterterrorism method is related to psychoanalysis of terrorist personality to better understand ideological and psychological aspects.

To this effect, IMCTC held, December 9 of 2021, a seminar at the IMCTC headquarters in Riyadh, featuring REAL ANALYSIS OF PERSONALITY TRAITS AND PSYCHOLOGY OF EXTREMISM, by Dr. Turki Mohammed Al-Atyan, Professor of Psychology at Imam Muhammad bin Saud Islamic University, and Dr. Hamid Khalil Al-Shayji, Professor of Sociology at King Saud University. The seminar was moderated by Dr. Abdullah Saeed Al-Dawh, Department of Ideology at IMCTC. Attendees included IMCTC Secretary-General, delegates of the IMCTC of member countries, and IMCTC staff and personnel.

Personality Traits

Dr. Al-Atyan provided an analysis of terrorist personality and presented the types of mental disorders common among terrorists (schizophrenia, bipolar syndrome, and paranoia). He further explained that paranoia is the most prevalent among terrorists. Therefore, one finds that terrorist personality is characterized by traits that revolve around paranoia, including:

- Displays ideological illusions that only occur in one's imagination and displays the ability to make up many illogical and unrealistic thoughts and events.
- Displays a propensity to quarrel and exaggerate grievances, fundamentalist religious fanaticism, blaming others for one's lack of self-efficacy and everyday life.
- Displays a very pathological jealousy of others, does not trust them, expects harm from others, and is always looking for signs and evidence to support one's fanatical ideas.
- Displays stubbornness and aggressiveness, and shows a propensity to argue and quarrel, criticizes others, and raises issues against them.
- Appears to others to be ambitious, of high-energy, and unwilling to compromise.

Thinking Methods

Al-Atyan also discussed terrorist key thinking methods, and how they manifest themselves in one's behavior:

- Deep-seated and overwhelming fear, and sense of failure and frustration, which lead terrorists to uncontrolled behavior that gives vent to one's desires and proves one's existence.
- Persistent intense anger, expressed by aggressive behavior towards society and individuals.
- The feeling of loss of identity and inferiority, and the feeling of guilt, which leads terrorists to develop a feeling of hate and despair in life, making terrorists take revenge by killing, destroying, sabotaging, intimidating and spreading terror.
- Bragging and a sense of pride, boasting about one's perverted abilities, and bravado, flexing muscles. Therefore, one will find that such terrorists may assume a nickname of great companions or change one's appearance of clothes in a special fashion.
- Following a method of thinking based on illusions and imagination, so one's ideology that manifested in one's behavior becomes irrational and illogical and does not agree with reality.
- Own thinking method depends on enthusiasm and impulsiveness, distorting facts and criticizing everything in society, while exaggerating petty mistakes, affecting such terrorists with a defect in their relationship with others, reducing them helpless to adapt, and unable to perform one's functions in the family, work and life. One always finds such terrorists in conflict with the values of society.
- Ignorance of truth; terrorists believe that their opinions and ideas, what he perceives and understands, and their actions are all natural. Such terrorists do not think that they have defects in their thoughts, feelings and behavior; rather, they see that their problems are caused by others.
- Their method of perceiving and thinking leads them to feel failure and frustration, so he or she suffers from severe psy-

chological disorder, locked in loneliness and isolation, and their desire for revenge constantly increases.

Rehabilitation of Terrorists

Dr. Al-Shayji discussed reintegration of violent extremists into society and presented the obstacles to social action with prisoners of violent extremism. Those released face many challenges; some of which are related to the prisoners themselves, and some others are attributable to society. Al-Shayji spelled out that the most important of such challenges, especially in cases of violent extremism, is social stigma attached to a given released person, and may prevent such individuals from returning to a normal social life.

Al-Shayji analyzed recent social trends in working with those who were involved in acts of ideological extremism, violence and terrorism, after their repentance and release. He presented his theory that he developed to qualify and help them integrate into society. Al-Shayji named his theory Five-Type Model Theory, which symbolizes the types of individuals that these people will meet in their social environment: (compassionate, admonitory, skeptic, glorifying, and observer).

1. Compassionate

The term refers to the nuclear family circle, surrounding a released individual; that is, one's close family members who love him or her, but will exercise a very close control over him or her, for fear of losing him or her again, slipping into the previous path. This is true because the bridge of trust between him or her and them has been shaken because of unacceptable behavior.

The vast majority of those who joined terrorist organizations or who slipped into conflict areas did so without the knowledge of their families. This situation eroded confidence. As such, the family members deal with them in such a manner that is different from the previous one, and they may clamp down on their movements and communication with others, which may lead to a reckless or unwise reaction from one's sons and daughters. The trust that has been shaken needs a short time to be rebuilt, thus comes the importance of enlightening both sides of the relationship to understand the situation and deal with it knowledgeably and wisely, so as not to lead to tense situations and undisciplined reactions, affecting the bonds of the family relationship.

2. Admonitory

It is the second circle, that is, members of the extended family of a released person, such as grandparents, uncles, aunts and seniors of the family. Some of them may blame and admonish him or her for what he or she has done, flooding them with questions, such as: Why did you bring us shame by your disgraceful act? The problem lies in the reaction, which may be negative, reckless or undisciplined, such as clashing, or cutting off communication, which impedes the process of integration and adaptation again with society.

3. Skeptic

It is the third circle, that is, people from the social environment surrounding a released person; such people may be former friends, neighbors, colleagues or classmates. Whenever such people see a former terrorist, they would run away or avoid talking to him or her. Such negative attitudes, behaviors and inferior views of a repentant terrorist, by people who know him or her, are supposed to be helping him or her to overcome his or her crisis and facilitate his or her reintegration into society again, may hinder his or her adaptation and smooth integration into society.

4. Glorifying

It is the fourth circle: people who are from the five most dangerous categories; they want to re-recruit or use former terrorists to recruit others, and they glorify his or her previous terrorist acts, and promise him or her compensation and revenge for those who harmed or stigmatized him or her. With this in mind, some repentant terrorists can be re-recruited, and they are drawn into extremism and terrorism again.

5. Observer

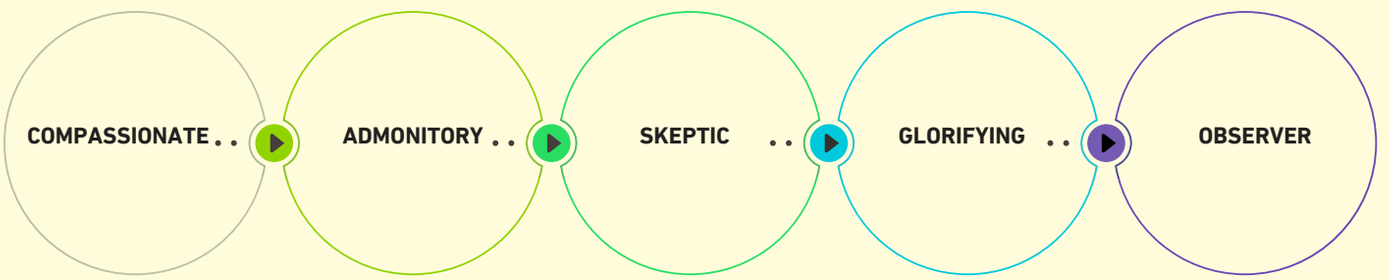
Security authorities monitor such terrorists after release to reach certainty that such former terrorists will stay away from deviant behavior and corrupt ideologies. Security authorities seek to help such former terrorists adapt and integrate into society, protect them from slipping back into deviant acts, and save them from communicating with deviant groups. The result of prison life is a refusal to monitor and follow up; they limit their freedom, which may push them to undisciplined reactions and behaviors that may hold them legally responsible.

Discussions

Discussions and inquiries about some aspects of terrorist personality followed the presentation and were brought to focus. Brigadier-General Rashid Al Dhaheri, Delegate of the UAE to IMCTC, asked about the scientific point of view in the psychology of lone wolves. Dr. Al-Atyan replied that the most prominent aspect of the personality of lone wolves is the ideological aspect. This personality moves towards a terrorist act without an organizational link, but with an ideological motive; this is what makes it difficult to control terrorist lone wolves.

Dr. Zayed Al-Harthy, Delegate of the Kingdom of Saudi Arabia, further explained the importance of distinguishing between the psychology of extremism and the psychology of terrorism; not every terrorist is an extremist, not every extremist is a terrorist, and not all terrorists are psychotic or mentally unhealthy. Some are normal individuals who have been deceived.

Al-Harthy also stressed the multiplicity of inputs to terrorism, being unlimited to ideology. The emotional side, for example, is no less important than the ideological side. Al-Atyan commented that his long experience in training terrorists confirms that no single terrorist is normal.



FIVE-TYPE MODEL THEORY

TERRORISM AND INTERNAL SECURITY CHALLENGES

Terrorism per se is one of the most notoriously despicable crimes that have plagued governments, societies, and cultures. Infamously instrumentalized and weaponized, terrorism has become a pretext for international intervention, which has helped to dismantle and destabilize some states. Therefore, the important roles of the armed forces in ensuring the unity and stability of the states are more critical than ever by countering terrorism and protecting national security, which has become a multi-faceted concept that encompasses several key factors, such as political stability, the rule of law, and the coherence of politics and security.

To this effect, IMCTC held a keynote lecture, featuring TERRORISM AND INTERNAL SECURITY CHALLENGES, by Brigadier-General Tariq Ahmed Koko Al-Taher, Delegate of the Republic of Sudan to IMCTC, December 13 of 2021. Relevant to the discussion were the concept of terrorism, root causes, the UN counterterrorism policy, the UN executive action plan of counterterrorism, the role of the armed forces in internal security operations, and the future view of terrorism in light of the existing reality.

UN Counterterrorism Policy

Koko presented the concept of terrorism, the differences between researchers, specialists and politicians in developing a specific and clear definition of terrorism, and how the description given by the media to members of terrorist organizations varies according to the political position they stake out, or the position of their countries and governments; they are terrorists, saboteurs, dissidents, criminals, soldiers of liberation, militants, or revolutionaries.

Koko walked the attendees through the root causes of terrorism alongside various manifestations, and a plague of economic, political, social factors, and religious factors, interlinked with the domino effect coming into play. More so, Koko also analyzed the sources of external and internal threat in the country that could give terrorism a foothold.

As the discussion progressed, the focus was shifted to the UN counterterrorism policy, the UN executive action plan thereof, and seminal function in supporting the countries to counter terrorism in perfect harmony with the streamlined international standards. The UN counterterrorism policy included four key pillars:

- Addressing the conditions conducive to the ubiquity of terrorism.
- Measures of counterterrorism and prevention.
- Measures of capacity-building of states to prevent and counter terrorism and strengthen the UN relevant roles.
- Measures to ensure respect for the human rights of all and the rule of law as the fundamental basis for counterterrorism.

The policy contained a number of important principles, including:

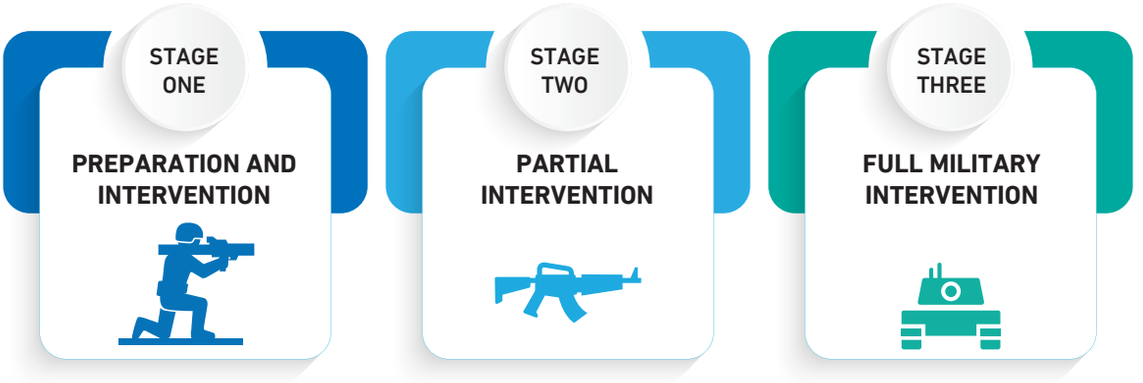
- Emphasizing that all terrorist acts of various manifestations are activities aimed at undermining human rights, basic freedoms and democracy, and destabilizing legitimate governments.
- Terrorism may not be associated with any religion, nationality, civilization or ethnic group.
- Recognizing that development, peace, security and human rights are interlinked and mutually reinforcing issues.
- Placing a special emphasis on addressing the conditions leading to the spread of terrorism, and taking urgent measures to prevent and counter terrorism, while recognizing that none of such circumstances can be a pretext or justification for acts of terrorism.
- Strong, unequivocal and continued categorical rejection of terrorism in all forms and manifestations, whoever commits it and wherever it is committed.
- Recognizing that international cooperation and any measures undertaken by states to prevent and counter terrorism must comply with relevant international conventions and rules of action and cooperation.

The UN action plan of the UN counterterrorism policy is devoted to preventing violent extremism and addresses the impact of violent extremism on peace and security, sustainable development, human rights, the rule of law, and humanitarian action. To this effect, it analyzed the context of violent extremism and associated drivers visible in the conditions conducive to violent extremism and the methods for the ubiquity of radical ideology and provided a program of action and useful recommendations on preventing violent extremism at the national, regional and global levels.

Roles of Armed Forces

Koko analyzed the roles of the armed forces and the tasks they are entrusted and mandated with in internal security operations. He spelled out that the main task of the armed forces is to defend the state, preserve the integrity of territory, waters, and airspace, within its territorial borders, provide protection from any external aggression, and maintain security and stability.

The armed forces are an integral part of the national security to defend the entire country from any external threat; they are a safety valve on which the security services rely in maintaining security and stability at the internal level. In normal cases, the armed forces usually perform secondary tasks to support gov-



THE STAGES OF USING THE ARMED FORCES IN INTERNAL SECURITY OPERATIONS

ernment efforts in stability and security internally. However, it may sometimes require the intervention of the armed forces to support the civil authorities in restoring internal security, enforcing law, providing military assistance in confronting demonstrations associated with violence and riots, or insurgency and civil disobedience accompanied by terrorist acts, confronting public disturbances and chaos, and supporting civil society in disaster relief action.

For further elaboration, Koko divided the stages of using the armed forces in internal security operations into three stages. First Stage is preparation and intervention. Stage Two is partial intervention when threat develops into a stage that decreases the policing ability to confront and control it, thus becoming helpless to face the situation. Stage Three is full military intervention, when threat increases and foretells the collapse of law and order, and the policing forces completely lose control of security.

The authorities to issue orders for the armed forces intervention differ according to each stage. In the case of complete intervention, the higher political authority in a given country is responsible for issuing intervention orders; in the case of partial intervention, the order is issued by the joint operations center of the armed forces after obtaining approval by the supreme military authority. In all stages of intervention, the armed forces abide by the rules of use of force and weapons, primarily maintaining composure, and using means of persuasion and warning before using force, including the use of light and medium weapons in accordance with an order issued by the higher military authority and when the forces are endangered by direct fire.

In conclusion, Koko presented a future view of terrorism, in which he called for supporting the capabilities of the counterterrorism agencies, sharing relevant information, and raising the efficiency of social institutions in counterterrorism.

IMCTC and International Response

General Raheel Sharif, Military Commander of IMCTC, emphasized the importance of historical, geographic and developmental aspects in counterterrorism, and the need to return to normality after counter-terrorism operations and the importance of the international response to counterterrorism. Sharif spelled out that IMCTC, empowered by various initiatives, is undoubtedly one of the most prominent types of this response.

Brig Gen. Raed Saleem Al-Marashda, Delegate of the Hashemite Kingdom of Jordan, called for a differentiation between internal security operations and counterterrorism operations; not all operations to restore security and order are counterterrorism operations. Demonstrations and sit-ins are not manifestations of terrorism, but if they are not addressed, they may open up Pandora's box to terrorism. The causes of terrorism are complex and overlapping. Internal causes may grow with external support. More importantly, internal security and stability are critically vital. The armed forces should not be used in internal security except for an urgent necessity and for a short period of time; deploying the army into the streets gives a negative impression of the country abroad.

Lieutenant-Colonel Hamid Karim Baig, Delegate of Pakistan to IMCTC, highlighted the importance of comprehensive training of personnel in counterterrorism units, not limited to military aspects only; such training includes psychosocial aspects, as well.

COMPARATIVE STRATEGIES FOR COUNTERTERRORISM

It is no secret that terrorism per se is a global threat to peace and security; it notoriously enervates countries, communities, and culture widely. To nip it in the bud, the world has spared no effort in counterterrorism, by following various strategies at the national, regional and international levels. To this effect, IMCTC held a keynote lecture, featuring COMPARATIVE STRATEGIES FOR COMBATINGTERRORISM, by Dr. Farhat Al-Harshani, Advisor to IMCTC, December 15 of 2021 to better provide a clear-cut explanation for the said strategies.

Refining Concepts

Dr. Farhat Al-Harshani provided an explanation for the concepts of strategy and terrorism. He pointed out that the concept of strategy is one of the oldest known concepts. It first appeared in the military domain. As human development and growth of international and economic capabilities, the concept of strategy was introduced to various fields, primarily to politics and sociology. The use of the term progressively developed and was introduced into all fields and human activities.

The concept of strategy now has two directions. Direction One is the specialized strategy that represents the investigation plan for the objectives of a specific activity from the government sub-activities, such as education, security and economy. Direction Two is the holistic strategy that represents the plan based on achieving political goals in general, whether in peace or war.

By the same token, the concept of terrorism currently has two directions. Direction One defines terrorism and objectives. Direction Two defines terrorism by content or means; the use of terror and violence, regardless of any goals.

The international community has not yet adopted one holistic definition of terrorism. Different definitions are provided in many partial agreements, such as the Geneva Convention for the Suppression of Terrorism within the League of Nations of 1937, and numerous texts in the United Nations General Assembly or the International Security Council between 1994 and 2004, and in regional agreements, such as the Arab Convention Against Terrorism of 1998, and the Convention of the Organization of African Unity to Prevent and Combat Terrorism concluded in 1999.

In all such provisions, the definition of terrorism was based on the criterion of content, and not on objectives. Terrorism is defined by the Arab Convention as "every act of violence or threat, regardless of motives or purposes, in the implementation of a criminal project, collectively or individually, aimed at spreading terror, intimidation, or harm among people, or endangering their lives, freedom or security, or causing damage to the environment or a public or private facility or property, or occupying or seizing it, or endangering a national resource."

Al-Harshani distinguished between terrorism and similar concepts, such as extremism, political violence, organized crime, and armed resistance. He concluded that it is difficult to define terrorism; there is no general international agreement about it.

Counterterrorism Strategies

Since terrorism has snowballed into reality, the international community has approved various counterterrorism strategies, at the national, regional and global levels. Al-Harshani analyzed some strategies, such as the UN Global Counterterrorism Strategy, approved by the international organization in 2006, coupled with an action plan, and based on four bedrock principles to address the conditions conducive to the spread of terrorism, prevention and counterterrorism, and strengthen the relevant efforts made by the UN. In this regard, ensuring respect for human rights and the rule of law is the basis for counterterrorism.

The Global Counterterrorism Strategy is a living document; it is reviewed by the UN General Assembly every two years. It is designed to adapt to the priorities of the member states in counterterrorism. It is also a holistic tool to support counterterrorism efforts at the national, regional and international levels and includes concrete actions to be taken nationally or internationally to prevent and counter terrorism.

The European Commission (EC) also adopted the EU Counterterrorism Strategy 2020, which includes counterterrorism, organized crime, detecting and preventing mixed threats, and increasing the resilience of critical infrastructure to strengthen digital and cyber security, support research and innovation, protect Europe from terrorism and organized crime, and strengthen the action of governmental and non-governmental institutions to counter ground attacks, counter cyber-attacks, disinformation campaigns, fake news and hate industry.

The Council of Arab Interior Ministers adopted the Arab Strategy for counterterrorism in 1997 with the aim of strengthening and coordinating the counterrorism efforts of the Arab countries. The strategy includes the basic lines of counterterrorism in the Arab countries, aiming at counterterrorism and eliminating root causes, main-

taining the security, safety and stability of the Arab countries, and the foundations of legitimacy and the rule of law. The strategy is concerned with strengthening and developing cooperation between the Arab countries and supporting counterterrorism cooperation with countries and international organizations. For proper implementation of the strategy in each country, the strategy urged the Arab countries to commit to establishing a national counterrorism committee, formed by representatives from the relevant agencies, and to establish a specialized unit to collect information on terrorist acts.

National Strategies

Dr. Farhat Al-Harshani addressed a set of national counterterrorism strategies in comparative analysis. He spelled out that the Kingdom of Saudi Arabia has adopted a holistic, multifaceted and integrated counterterrorism strategy, based on three pillars: prevention strategy, treatment strategy, and care strategy.

Prevention strategy aims to support the efforts that seek to foster the community awareness about the threats of extremist, deviant and misinformed thought, promoting moderation, correct misconceptions, and combat the ideologies that feed extremism.

Treatment strategy draws on a set of measures, including re-education and enlightenment programs, advice, guidance, and counseling. Care strategy includes interaction with those who have been released and their families, providing them with financial and moral support, organizing rehabilitation programs to help them to adapt again to the requirements of the Saudi society, finding job opportunities, stability and full integration into society.

The Moroccan counterterrorism strategy is based on an integrated and coherent approach, based on the promotion of the values of moderation, tolerance, human rights, and the consolidation of the rule of law. It also includes the adoption of measures aimed at combating poverty and exclusion, achieving social equality, and supporting and integrating extremist prisoners and former prisoners.

The Tunisian counterterrorism strategy was developed according to a multi-faceted global approach, based on the global counterterrorism strategy, and on several successful regional and national strategies. It aims to isolate terrorism from its feeding associations and develop counterterrorism methods by going beyond the security and military fields, while ensuring balanced and robust engagement between all the authorities and institutions concerned.

The United States of America issued more than one counterterrorism strategy given the many US presidents and their different policies. The latest strategy, October 4 of 2018, developed the ultimate goal of defeating terrorists who threaten the US security, preventing future attacks, and protecting national interests. The US strategy included six key areas:

1. Continued pursuit of terrorists.
2. Drying up sources of support for terrorists.
3. Updating the US counterterrorism authorities and relevant tools.
4. Protecting the US infrastructure and enhancing resilience.
5. Countering terrorist extremism and recruitment.
6. Strengthening the counterterrorism capabilities of the US international partners.

IMCTC Strategy

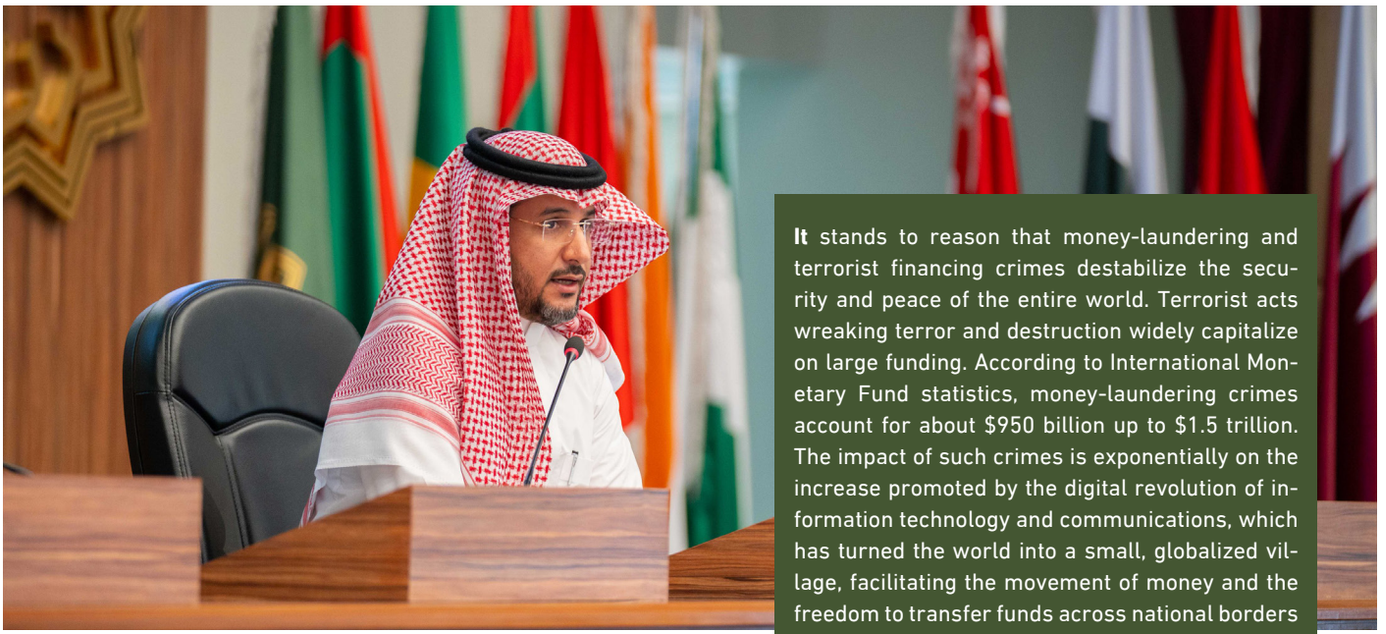
Dr. Farhat Al-Harshani also analyzed the IMCTC strategy, considering its relevance to international and national strategies. He also spelled out that IMCTC followed a vertical plan according to the following domains: ideology, media and communication, combating terrorist financing, and military, which intersect and overlap with international, regional and national strategies. Each domain (except for military) necessarily contains a preventive, protective and deterrent aspect. The IMCTC strategy goes in perfect harmony with the various strategies. The IMCTC action is concerned with the important components upon which every terrorist act is orchestrated, regardless of means: ideology, money, media, and military.

Conclusion

Al-Harshani drew a seminal comparison between the national, regional and international counterterrorism strategies and developed a set of key conclusions:

1. The said strategies are similar in several points. Although recommendations are differently developed, they all declare war on terrorism. All the strategies operate in concert to combat extremism as a pathway leading to terrorism, especially as it is the cornerstone for the formation of a fanatic and violent personality, before joining terrorist groups.
2. All global and regional counterterrorism strategies emphasize the importance of international relevant cooperation; terrorism has become a cross-border phenomenon that snowballs and balloons into everywhere. Terrorism is notoriously rampant across porous and poor borders and war-torn areas, which lack security and are infamously riddled with insurgencies. The strategies unanimously link terrorist crime with transnational organized crime.
3. Global and regional counterterrorism strategies focus on modern terrorism or cyber-terrorism, with a new terrorist generation that is educated and empowered to use the state-of-the-art technologies and sources of information to attract recruits and organize terrorist operations.
4. National strategies in various countries are inspired by global and regional strategies, so they are not different in general. They are similar in the basic counterterrorism objectives, but they differ in some means given the different capabilities and circumstances of each country.

FINANCIAL INVESTIGATION OF MONEY LAUNDERING AND TERRORIST FINANCING CRIMES



It stands to reason that money-laundering and terrorist financing crimes destabilize the security and peace of the entire world. Terrorist acts wreaking terror and destruction widely capitalize on large funding. According to International Monetary Fund statistics, money-laundering crimes account for about $950 billion up to $1.5 trillion. The impact of such crimes is exponentially on the increase promoted by the digital revolution of information technology and communications, which has turned the world into a small, globalized village, facilitating the movement of money and the freedom to transfer funds across national borders through widespread, fast-moving, and extremely complex financial systems.

To this effect, IMCTC organized, on December 22 of 2021, at the IMCTC headquarters in Riyadh, a keynote lecture, featuring PARALLEL FINANCIAL INVESTIGATION PROCEDURES IN MONEY-LAUNDERING AND TERRORIST FINANCING CRIMES by Mr. Ahmed Mohammed Al-Muqhim, Prosecutor of economic crimes and a co-founder of the Money-Laundering Unit at the Public Prosecution of the Kingdom of Saudi Arabia.

Socioeconomic Threats

Al-Muqhim emphasized that money-laundering and terrorist financing crimes are a grave threat to the socioeconomic aspects of any given country, especially countries suffering from poor countermeasures of such crimes.

Economically, such crimes tarnish the reputation of any financial systems, while depriving a given country of important financial resources that can be appropriated for employment and development, raising inflation rates, and affecting the rules of fair and honest competition.

Socially, the failure to prosecute the proceeds of crimes enables perpetrators to exploit such proceeds to fuel crimes and finance terrorism. The spread of money-laundering operations in any society increases crime rates and declines the values of education and culture.

Similarities and Differences

Al-Muqhim discussed the similarities and differences between money-laundering crimes and terrorist financing crimes, spelling out that both typologies feed on concealment and deception, and require international strategic cooperation, due to their cross-border ubiquity. Such crimes need a supervisory treatment and financial investigation procedures. On the other hand, there are many differences between the two types of crimes in several key aspects, such as:

- **Source of Money:** Money-laundering crimes draw on illegal sources; such money comes from criminalized sources (drug trafficking, antiquities smuggling, contrabands smuggling, human trafficking, etc.), while the terrorist financing can be funneled through legitimate and illegitimate sources.
- **Volume of Money:** Money-laundering crimes involve big money, not comparable to money-laundering crimes of terrorist financing.
- **Goal:** The goal of money-laundering crimes is to make financial profits, while the goal of terrorist financing is to gain political or ideological progress.
- **Method of Money Movement:** Money in money-laundering crimes move through financial institutions in a circular manner, starting and ending with a money-launderer. Funds of terrorist financing may not follow the path of financial institutions and take a linear path that begins with a financier and ends with a terrorist organization.
- **Scope of Detection:** In money-laundering crimes, detection focuses on identifying the relationships between the individuals involved in a given crime. In terrorist financing crimes, the focus is placed on money and associated movement.

Al-Muqhim reviewed the key methods of concealing funds in crimes, such as digital transactions, which have become a notoriously dangerous means, inter alia, used by criminals, and instrumentalizing goods that have no standard for their value nor control over their prices, such as antiquities, paintings, and establishment of fictitious companies, and the customs declaration claiming that a person has money, and is given a clearance of claimed funds to use and deposit suspicious funds, divide funds, such as opening more than one bank account, or transferring money to more than one beneficiary, using large fake contracts and supplies, and funneling funds.

Parallel Investigation Role

Al-Muqhim discussed the parallel financial investigation and the vital role in combating money-laundering and terrorist financ-

ing crimes. He spelled out it collects material financial evidence by identifying financial transactions of suspects, and financial movements to learn about the proceeds of the original crime and the crime of money-laundering, means, and seize, or flagging up and tracking such money, and providing the evidence necessary for investigation, indictment, detention and confiscation. In one of its recommendations, the FATF states that governments should conduct a parallel proactive investigation with regard to all cases of money-laundering and terrorist financing, and the associated predicate crimes. Simply put, the court, as it initiates an investigation into one of the predicate crimes believed to be related to financial proceeds, opens a financial investigation parallel to the criminal investigation, during which it searches for and tracks the financial proceeds of such a crime and provides evidence to link these financial proceeds to the original crime.

The success of parallel financial investigations in recovering proceeds of crime is taken as an important criterion for identifying how compliant a given country is with the requirements of combating money-laundering crimes, and a key factor contributory to global assessment, thus removing it from the list of high-risk countries.

A parallel investigation is proactive; it identifies the proceeds of crime under investigation, prevents illegal profits from penetrating the economy, thereby removing the instruments of future crime, and reinforces the important principle in law and society that no one benefits from crime.

Financial investigation and parallel financial investigation are critically important given their vitals roles in identifying and documenting the movement of money. They both identify the motives and connections between the people involved, reveal all participants in a given criminal act, and the organizational structure of criminal organizations, identify the threat of each individual accused, monitor the proceeds of crime under investigation, and help uncover crimes. They also identify the locations of suspects, witnesses, victims, the means and methods used in such a crime.

Investigation Methods and Sources of Information

Al-Muqhim presented the key methods used in parallel financial investigation, and the relevant sources of information, pointing out that some methods follow secret procedures, while others follow open ones. Secret-path key procedures include:

- Field research and investigation, by movement, inspection, and in-field observation.
- Secret operations, in which a criminal police officer operates in disguise as a man who practices the same activity as a given accused and meets with the target person to learn about the dimensions of a given crime, and the parties involved. Officers of criminal justice who perform such tasks usually undergo extensive training until they perfect stealth skills.
- Controlled delivery, by letting a tracked accused person continue their activity (e.g., delivery of drugs), so that all those involved in a given criminal network can be spotted and arrested in flagrante delicto and ensure their conviction.
- Monitor communications, after obtaining the prosecution's permission, to monitor the defendants' communications and their internal and external relations.
- Writing to the competent authorities to find out what such a given accused person has.

The key investigation methods that follow open procedures include requesting a given accused to bring documents that prove the source of their money, informing the criminal investigation officer in charge of the banknote financial document, and discussing and confronting such an accused person. Key sources of information in parallel financial investigation include:

- Criminal information, which is the criminal record that identify the history of a given accused person.
- Digital devices which a given accused person has; they are one of the most important and powerful sources of information. Criminal investigation officers must take the initiative to obtain the information contained in such sources before they are deliberately damaged or sabotaged.
- Financial information in financial institutions, such as banks and money stock exchanges.
- Classified information, which is related to the security aspect of the security services.
- Regulatory information held by regulatory authorities, such as industrial and commercial bodies, customs, passports, and others. It includes information that can disclose important aspects and activities of those accused of money- laundering and terrorist financing crimes.

Discussions

Several discussions and questions were raised by the delegates of the IMCTC member countries. Brigadier-General Nawaf Al-Jutaili, Delegate of Kuwait, asked for further explanation about the indications of money-laundering and terrorist financing crimes. Al-Muqhim spelled out that the supervisory institutions have indications thereof, such as financial movement not proportional to the income. Brigadier-General Rashid Al Dhaheri, Delegate of UAE, asked about the exploitation of famous social media applications in money-laundering, and how can this be followed up and addressed? Al-Muqhim replied that those involved in money-laundering and terrorist financing crimes are always quick to devise new methods for such crimes, including targeting famous social media platforms, because there are no standards or controls for their money. As such. It is critically important to document their money and regulate advertisement content on their pages. To this effect, the Kingdom of Saudi Arabia has taken relevant steps.

HACKING AND PREVENTION METHODS

HACKER SCREEN REAL EXAMPLES

Cyber intrusions known as hacking are one of the most serious threats that bedevil and harry internet users, whether governments, institutions or individuals. Triggered by hacking, extortion, theft, and many other crimes have become notoriously instrumentalized. Such disruptive activities can cut off services, destroy property, and remove data. More so, wars are expected in the near future to snowball into cyberspace, which is the cheapest, easiest, fastest and most efficient modality of warfare. To have a foresight to better understand the threats and prevention methods, IMCTC held, October 27, 2021, Riyadh, a keynote lecture, featuring HOW HACKING OCCURS? REAL EXAMPLES FROM A HACKER'S SCREEN, co-presented by Dr. Basil Al-Sadhan, Associate Professor of Network Security at the College of Engineering at the University of King Saud and Engineer Abdullah Al-Qahtani, Member of the Information Security Association, Cyber-Security Department in the Kingdom of Saudi Arabia. Among high-profile attendees were Secretary-General of IMCTC, delegates of the IMCTC member countries and staff.

Cybersecurity

With many cyber intrusions ubiquitously ballooning into reality over the recent years; it has become necessary to have strong defense and protection that can confront these destructive operations, which has come to fruition through cybersecurity. Interestingly enough, one may wonder why we squander billions of dollars on conventional weapons, when a hacker can potentially disable a multi-million-dollar aircraft carrier through a clickable action on a handheld computer, sabotaging the infrastructure of digital governments or hack and disable the data and devices of ministries of sensitive security!

The two keynote speakers addressed the types of computer technical intrusions, modalities, and best practices for protection and prevention. They further explained the concept of cybersecurity; one of the branches of modern technologies, concerned with protecting networks, information technology systems associated components, services, and data, including penetration or disruption. Cyber-attacks usually aim to gain access to sensitive information to alter, damage or extort and force users to pay money. The concept of cybersecurity includes information security and digital security. Cybersecurity is critically important for the following reasons:

- Confidentiality: only authorized persons can access information.
- Safety: verification of information when entered, preserved, or transmitted; this includes protection from sabotage attacks or theft.
- Availability: the information owner can access information when needed at any time; methods are made available to recover data in the event of a breach or disaster.

Therefore, cybersecurity is a real challenge for organizations given the rapid development of technologies that must be protected alongside the threats that arise in unison with these technical developments, and the large number of security solutions being developed to address such challenges. Taken together, it requires a thorough and deep understanding to implement new solutions in an integrated and faultless manner, consistent with other technical and security solutions in use.

Cyber Attacks

Cyber-attacks mean malicious activities carried out by individuals or institutions to cause a dysfunction to information systems. Attackers usually penetrates the victim's network when a favorable opportunity arises. Key categories of attackers include:

Script Boys: They are inexperienced people who use ready-made tools to defame websites, gain admiration, and seek self-actualization.

Hacktivists: They are like script boys, but they are politically motivated.

Cybercriminals: They target commercial businesses, banking services, and credit cards to blackmail and make money.

Government-Funded Individuals: They are the biggest danger;

they can employ the best talent to carry out advanced attacks in a stealth fashion, and sometimes even design customized attacks, making it very difficult to protect such targets.

Real Examples of Cyber Attacks

The two keynote speakers also addressed the key models of cyber-attacks as exemplified:

Ransomware

Ransomware is a malware program that prevents a user from accessing their systems or personal files. Ransomware pretends to be useful to convince the victim to download it, then targets the operating system and encrypts all data stored on the device to force the victim to pay a ransom for decryption, usually in Bitcoin.

Sometimes hackers set a time to pay the ransom no more than three days, otherwise the amount will double or else remove the data. Prompted as such, the victim rushes into succumbing to the hacker's requests. There are several methods to send ransomware to the victim's PC, such as malicious ads, spam emails, and installing risky applications. Ransomware is a major threat to all organizations and institutions. A report issued by SOPHOS, cybersecurity company, reveals that ransomware has invaded more than 150 countries, including Germany, Austria, Switzerland, the United States, the United Kingdom, and Canada. More than two hundred thousand victims of institutions and individuals have been traumatized.

Trojans

Metaphorically, Trojan connotes deception and fraud; it is a software program that pretends to be harmless to convince the victim to download it on their device. The real purpose is for the hacker carry out harmless actions onto the target device, such as spying on the contents of the device, stealing, removing or destroying data, or completely destroy such target devices. Hackers can download trojans as a service for dollars, or for a monthly subscription fee, and then redirect it to individuals and companies in a malicious e-mail or documents. Trojan works as a digital worm that infects various applications and software systems.

Social Engineering

Social engineering psychologically tampers with people; the use of deception to decoy and lure someone into revealing confidential or personal information. Social engineering relies on the human dimensions; anyone with some savvy can do this task, regardless of the two-way interaction, or a deep knowledge of modern technologies. Social engineering is often carried out by phone or e-mail, impersonating an important person, enabling the fraudster to ask personal questions without arousing suspicion by the victim.

Disrupting Distributed Services

They are commonly referred to as denial-of-service attacks; it is an attempt to make network resources unavailable to their legitimate users, whether by a single device or an army of devices. It violates device resources, such as CPU, memory, network bandwidth, and energy savings (battery). It prevents the provision of services. Such attacks act like a person constantly calling a phone line to keep them busy and prevent others from calling. It can disrupt and deny the service for a long time.

Phishing

Phishing is an increasingly common cybercrime; phishing causes a great impact on the desired goals. The hacker seeks to send fraudulent types of communications that appear to be from a trusted source, often via e-mail. Through phishing, sensitive data are stolen, such as credit card data, login information, or the installation of malware program on the victim target device. The hacker deceives the recipient of the message by giving them the information directly or doing something that enables the hacker to obtain such information.

Protection Methods

The two speakers explained the protection methods used to stave off such malicious attacks, including but not limited to the following:

- Constant updates of different operating systems and programs.
- Backing up important data.
- Using powerful programs to stave off against viruses.
- Updating the definitions of anti-virus programs.
- Disabling unused services on computers.
- exercising caution when installing unknown programs.
- Establishing policies that require the use of strong passwords.
- When ensnared, you must not comply with the demands of hackers; immediately stop all operations in the device or network and restore the backup copy.

The methods used to be protected from social engineering include but not limited to the following:

- Change passwords constantly; not to be shared with anyone.
- Avoid using one username and one password for several accounts.
- Avoid entering unsecured wireless networks.
- Do not leave computers unlocked.
- Verify who is contacted by phone, email, or social media.
- Avoid opening email attachments from unknown parties.

The two speakers also explained the protection methods used to steer clear of phishing, including but not limited to the following:

- Avoid opening and deleting messages directly.
- Activate the message filtering feature; it can delete unwanted messages.
- Do not open anonymous links; such links may lead to device hacking and data theft.
- Avoid messages that request personal information.
- Avoid opening files with untrusted extensions.
- Avoid entering suspicious websites.
- Ensure that programs and applications are downloaded from their official sources.

In conclusion, the two speakers presented methods to achieve best practices for cybersecurity:

- Provide the latest technologies.
- Rely on trained and qualified people to address competently and efficiently such, violations, breaches and intrusions.
- Develop integrated plans to address such disruptive practices.

IMCTC JOINS DELEGATES OF UAE, BAHRAIN AND LIBYA IN NATIONAL DAY CELEBRATIONS


United Arab Emirates' Delegate


Kingdom of Bahrain's Delegate


State of Libya's Delegate

IMCTC celebrated the National Day of three IMCTC member countries, December 2021, at the IMCTC headquarters in Riyadh. Attendees included Secretary-General of IMCTC, delegates of IMCTC member countries, and IMCTC staff and personnel.

The delegates of the United Arab Emirates celebrated, December 2, 2021, the 50 National Day in commemoration of the federation of the UAE in 1971, by Sheikh Zayed bin Sultan Al Nahyan, rest in peace. Later, on December 16 of 2021, the delegates of the Kingdom of Bahrain held a celebration in commemoration of the Kingdom's 50 National Day, which coincides with the Independence Day in 1971 and the 22 Anniversary of His Majesty King Hamad bin Isa Al Khalifa taking up the reins of power in the Kingdom of Bahrain. On December 26 of 2021, the delegate of the State of Libya held a celebration to mark the 70 anniversary of Libya's independence. The said anniversary is the culmination of the struggle and sacrifices of Libyans for long decades to have gained independence in 1951.

On this occasion, IMCTC expressed heartfelt congratulations to the leaders of countries and their peoples, wishing everyone continued progress, security and prosperity.

IMCTC SECRETARY-GENERAL RECEIVES THE MILITARY ATTACHÉ OF ARAB REPUBLIC OF EGYPT

Secretary-General of IMCTC, Major-General Mohammed Saeed Al-Moghedi, paid tribute to the counter-terrorism efforts made by the Arab Republic of Egypt in all forms and manifestations. The timely appreciation came in when he received the Military Attaché of the Arab Republic of Egypt to the Kingdom of Saudi Arabia, Brigadier-General Mohammed Naji Mohammed Youssef, at the IMCTC headquarters in Riyadh, December 30 of 2021. On his side, the Military Attaché highlighted the importance of continued cooperation with IMCTC to further share experiences and expertise in combating violent extremism and counterterrorism, commending the IMCTC relevant efforts.

HIGH-PROFILE DELEGATION FROM THE COLLEGE OF COMMAND AND STAFF IN RIYADH VISITS IMCTC

IMCTC received a high-ranking delegation from the Command and Staff College in Riyadh. The delegation was briefed on the IMCTC counterterrorism efforts, across four key domains: ideology, media and communication, combating terrorist financing, and military.

OPENING TRAINING PROGRAM FOR TEACHING ARABIC TO NON-NATIVE SPEAKERS

Secretary-General of IMCTC announced, December 12, 2021, the opening of the training program (TEACHING ARABIC TO NON-NATIVE SPEAKERS), at the IMCTC headquarters in Riyadh. Attendees included the delegates of the IMCTC member countries and IMCTC staff and personnel. Major-General Al-Moghedi explained that a wealth of faculty members at Imam Muhammad bin Saud Islamic University would conduct the said training program. Of great note, the training program aims to contribute to developing the capabilities of the delegates of the IMCTC member countries and enhancing their knowledge and language skills.