JANUARY EDITION 2021, NO. 23

متحالفون

MONTHLY BULLETIN ISSUED BY IMCTC

TWO MEMORANDA OF COOPERATION BETWEEN IMCTC AND NAIF UNIVERSITY AND FINANCIAL ACADEMY

IMCTC signed an MOC with Naif University, 23 December 2020. Major General Mohammed Saeed Al-Moghedi, Secretary-General of IMCTC, emphasized the MOC comes within the framework of the IMCTC efforts for joint cooperation and coordination with Arab, Islamic and international organizations and centers. Major General Al-Moghedi expressed his aspiration to further invest such cooperation between IMCTC and Naif University in a scholarly and methodical manner in research to better enhance the common vision and contribute to exchanging visits, information, publications and training.

His Excellency Dr. Abdul Majeed Al-Banyan, President of Naif University, commended the great counterterrorism efforts made by IMCTC, highlighting that such a partnership will better contribute to serving Arab and Muslim communities.

IMCTC also signed another MOC with the Financial Academy, 14 December, 2020. Mr. Manea Al-Khamsan, Director-General of the Financial Academy, paid tribute to the IMCTC counterterrorism efforts and supporting global actions aimed at maintaining international peace and security.

Major General Al-Moghedi also received, 17 December 2020, H.E. Ambassador of Bangladesh to Saudi Arabia, Dr. Muhammad Javid Battwari, to discuss avenues of cooperation and coordination.

IMCTC CELEBRATES UAE NATIONAL DAY AND INDEPENDENCE DAY OF LIBYA

In the presence of Secretary-General of IMCTC, Military Commander of IMCTC, delegates of member countries, and IMCTC personnel, Delegate of the United Arab Emirates to IMCTC, Brigadier General Rashid Mohammed Al-Dhaheri, held a celebration on 2 December, 2020 to mark the 49th National Day of the UAE. Brigadier General Al-Dhaheri commended the highly appreciated values deeply rooted in the conscience of the UAE people and the pioneering role played by the UAE, as it provides an exceptional model in development through scholarly and economic achievements that represent a quantum leap towards a better future for its people and for the Arab and Muslim nations.

In a similar vein, Delegate of the State of Libya to IMCTC, Brigadier General, Mustafa Ibrahim Ali Souissi, held a celebration, on 24 December 2020, to commemorate the Independence Day of the State of Libya. Brigadier General Souissi highlighted the importance of the occasion and its great symbolism to the Libyan people, stressing that his country is on the way to recovering from the ordeals that have befallen it; Libya will restore its position among the Arab and Muslim countries to contribute to achieving security, stability, reconstruction and development.

COUNTERMEASURES AGAINST CYBERTERRORISM IN CYBERSPACE

Dr. Saleh Al-Saad Miqdadi

Given the fact that cyberspace has infamously become one of the safe havens for terrorist groups, slithering into communities to instill their ideologies to trap and decoy more victims, the threat generated by cyberterrorism in the cyberspace via social media is no longer a clandestine activity; it has snowballed into a dire and serious threat to society, especially to the youth and the counterterrorism security services. The websites controlled by such terrorist groups have infamously expanded and sprouted up, luring thousands of individuals into their propagandas, narratives publications and news translated into twelve languages; this simply means that different groups of races, languages, religions and cultures are targeted to attract supporters and donors and to recruit more fighters.

RESOLUTE CONFRONTATION

It is critically important to gear up and counter such serious cyberterrorism. To this end, it has become imperative to take all necessary actions, measures and methods available by the concerned agencies, including security, media, awareness, technical, or other competent authorities, as each plays its vital roles to better monitor and track cyberterrorism activities accurately, by putting into action the following:

First: Media

Official and unofficial media should be empowered to directly confront websites that promote extremist ideology and terrorist behavior online in general, and on social media in particular. Media outlets can bring to the public the human and social aspects that awaken the individual and collective conscience, such as recalling the multitude and magnitude of victims perpetrated by terrorism, the despicable conditions and unbearable suffering of people bereaved by the scourge of terrorism and suffering, especially the vulnerable group, which constructs more efficient and meaningful messages voiced to the public. This also motivates security agencies and security media to better develop a plan for the security employment of social networks to confront extremism and terrorism, keeping their eyes widely open to suspicious websites, while enhancing cooperation between security media and other media at all national levels to nip in the bud violent extremist ideology that feeds cyberterrorism.

Equally important, clear controls for media should be adopted to closely follow up terrorist activity, taking into account a set of key must-do actions:

- A wealth of well-qualified, specialized media professionals should be authorized to follow up the media related to extremism and terrorism.
- Scrutinizing the materials published online by terrorist groups to lay bare such propaganda as they are reduced unreliable.
- Being cautious as not to exaggerate the dissemination of information and threats that terrorist groups publish lest it should impact people's attitudes, behaviors and beliefs, laying bare such activities in order not to daunt and reduce people's sentiment to marionettes.
- Highlighting the efforts of the competent security agencies in countering cyberterrorism, thus enhancing the confidence of citizens and society in the great efforts made by such security agencies.

Second: Education-Based Awareness

Fostering education-based awareness by developing a national plan for comprehensive awareness of all citizens and residents, especially the target groups, and sensitizing them to the various methods on which terrorist groups feed and capitalize to lure the youth into the ill-fated paths. Equally important, this also includes publicizing suspicious websites, and warning citizens against being involved in such cyberspace. All relevant bodies from the national media, security media, religious media, educational media, youth media, family and school should equally be engaged in putting this plan into action. Conducting in-depth research studies

into cyberterrorism and associated manifestations also comes into play as it highlights the grassroots contribution and cooperation with the relevant agencies.

Third: Technical Field

The technical field can be by optimized by a set of necessary practical procedures:

- Developing a specialized, highly qualified and well-trained working group with advanced cyber-competencies fully equipped with state-of-the-art technologies, concerned with the permanent censorship and monitoring of social media websites exploited by extremist groups to disrupt and block them, while approaching and addressing such terrorist activities through scholarly, psychological, and sophisticated and non-traditional methods.
- It is critically necessary for the competent security services to benefit from extremist and terrorist websites, as they are important sources of information; such sources should be investigated, analyzed, interpreted and predicted, and should be confronted with the same ideological and logistical level, and even surpassing them by using their weapons, methods, tools, and their own websites, understanding the relationship between terrorist groups and terrorist ideologies, plans and strategies, and the statements issued by such terrorist groups.
- Some well-trained and professional security personnel can infiltrate into such websites around the clock to completely destroy such websites and lay bare their plans, which can be supported by publishing a scientific, religious, logical and evidence-based counternarrative that best refutes and exposes their ideologies. Taken together, this can reduce their websites to useless: hacked rather than being hackers to the government websites.
- Creating several websites, carefully developed and designed scientifically, religiously, culturally, socially and psychologically, that impart moderation and tolerance to lay bare false and baseless claims in such a manner as to be an efficient tool to expose and refute all their mendacity, crimes and terrorism, while highlighting the sublime values of Islam.
- Coordination with different internet service providers to actively cooperate in reporting visible and tangible terrorist activities, especially those that include threats to vital installations and institutions or to individuals of high-profile figures.
- Coordination with the companies that own and control the various search engines, and communication platforms such as Google, YouTube, Yahoo, Facebook, Twitter to prevent terrorists from using these well-known websites to broadcast their extremist and terrorist ideologies.
- Keeping a watchful eye on online financing operations, and adopting strict control over certain suspicious websites that provide advertisements, propagandas and services in exchange for large funds; although they seem to function as normal websites, they are in reality outlets via which financing is funneled for extremist cells or terrorist groups.
- Enacting strict electronic laws and legislations to counter terrorism in all its manifestations, including the misuse of websites and social media, ensuring that all gaps that intensify cyberterrorism crimes are addressed and investigated on an evidence-based and cogent manner.
- Preparing specialists to develop and gain extensive security and judicial expertise and competencies, knowledge, know-how, savvy, skill and sagacity to investigate and analyse issues of extremism, violent extremism and terrorism in general, and cyberterrorism in particular and to enhance awareness and education of counterterrorism laws and legislations.
- Encouraging the conclusion of bilateral and multilateral agreements between countries with mutual interests, at the regional and international levels, related to crimes of cyberterrorism and countermeasures and treatment approaches, the exchange of information and experiences, including mutual legal assistance, and the extradition of accused people, suspects and criminals who have been found guilty.

THE DUTCH NATIONAL COORDINATOR FOR SECURITY AND COUNTERTERRORISM

THE NETHERLANDS ARM IN PREVENTING CRISES AND DISASTERS

National Coordinator for Security and Counterterrorism
Ministry of Justice and Security
POLICIJA
SIPA

The Netherlands spares no effort in countering terrorism. Among several other counterterrorism approaches adopted by the Netherlands is identifying and monitoring individuals potentially involved in terrorism, and ensuring the security of the targeted persons and buildings at risk. To this effect, the Organization of the National Security and Counter-Terrorism Coordinator seeks to protect and support the Netherlands, in coordination with government partners, the research community and the private sector, which all aim to ensure that the Netherlands' vital infrastructure is safe.

ROLE MODEL

The central government first had one organization to counter terrorism and maintain cybersecurity, national security and crisis management. Once the efforts of the said organization were coordinated and thus unified with the partners in the security sector, the Netherlands has become a safe and stable destination; its utmost concern is to prevent social unrest across the region, which can be achieved only with the cooperation of the various parties to address national security issues.

The agency of the joint program for the said organization includes measures aimed at preventing, tracking and combating potential terrorist threats to national security to the Dutch soil. With human oversight of functions related to crisis management, counterterrorism, risk assessment and cyber security, effective information sharing among all units of the work team structure can be ensured.

The participation of all other actors operating in the extra-government national security, such as local authorities, civil society organizations, scholars, and private companies, makes the approach comprehensive and multidisciplinary. In addition, the said organization has previously developed many programs in coordination with other agencies, such as the "Comprehensive Dutch Action Program to Combat the Terrorist Approach", and has provided regular reports directed to the government and economic sectors and to the general public, local authorities and private companies. Taken together, the Dutch model has become a milestone in the comprehensive approach to security in the international arena.

Bringing these tasks closer into a single organization makes the Dutch government more effective in these areas. The NCTV along with its staff fall under the responsibility of the Minister of Justice and Security, functioning in a similar way to a directorate-general.

TASKS AND GOALS

The main tasks with which the NCTV is mandated and entrusted are:

- Identifying, explaining, exchanging and assessing threats and vulnerabilities (their minimum, basic or critical), and developing counter measurements and approaches.
- Enhancing the resilience of vital sectors, structures and networks.
- Monitoring and protecting individuals, as well as vital agencies and sectors.
- Crisis management, coordination and communication.
- Ensuring cyber-security.
- Supporting international cooperation (the European Union, the United Nations, NATO, and the Organization for Economic Cooperation and Development).

ORGANIZATIONAL STRUCTURE

The NCTV has about 300 employees, in addition to an office with a number of departments; Department of Analysis and Strategy, Department of Counterterrorism, Department of Cyber-Security, Department of Resilience, Department of Control and Protection, and Civil Aviation Security, in addition to National Crisis Center and National Center for Operations Coordination.

In the event of a national crisis or of a supra-regional nature, the NCTV shall operate the Center's tasks supported by the National Center for Operations Coordination. The former coordinates the efforts of the authorities and the decision-making process at the central government level, and ensures that both the public and the concerned authorities are kept informed of all the details; while, latter coordinates the measures necessary to control the crisis. When a crisis occurs at the local or regional level, the interaction is with the regional or local authorities.

The NCTV is responsible for the National Counter-Terrorism Strategy, Cybersecurity, Homeland Security and Crisis Management, and ensures the participation of actors from different fields.

COUNCIL OF EUROPE COMMITTEE ON COUNTERTERRORISM

OVERSIGHT AND COMPLIANCE OF LEGAL INSTRUMENTS

The Council of Europe Committee on Counter-Terrorism (CDCT) is an intergovernmental body that pursues the goals of the Council of Europe on counterterrorism. Among the most important of these main goals is to oversee the legal instruments of the Council of Europe and to further ensure their accurate and successful application. The CDCT seeks to take the necessary methods and tools for international experts to better analyze developments in counterterrorism and evince efficient response accordingly.

The CDCT actions are in line with the international standards applicable to serve the set goals. To this end, the CDCT relies on the principles of prevention, prosecution and protection. Equally important, the CDCT has been mandated and tasked to develop effective tools for non-binding legal instruments; these tools are mainly represented in recommendations and guidelines proposed to member states for consideration, which are then put into action to counter terrorist activity.

In 2018-2019, the most important priorities of the CDCT were developing the Council of Europe's counterterrorism strategy from 2018 to 2022, and examining the feasibility of developing a legal definition of terrorism to be agreed upon by all European countries, addressing the phenomenon of foreign terrorist fighters and returnees, investigating the terrorist misuse of the internet, the impact of the participation of women and children in terrorism and the discussion of the relationship between terrorism and organized crime.

The CDCT provides a platform that provides information on the legislative and institutional counterterrorism in the member states, exchanges best practices and experiences and promotes effective implementation of the Council of Europe's legal instruments on counterterrorism. The Center assists in the appreciation of the member states to counter terrorism, committed to respect human rights and the rule of law. The Central Counterterrorism Committee and the European Court of Human Rights provide a regularly updated fact sheet on counterterrorism issues of the European Convention on Human Rights.

This also includes providing regional summaries of legislative and institutional counterterrorism, monitoring sanction and ratification, and overseeing the preparation of the European Court of Human Rights database on counterterrorism cases.

European Ministers of Justice called on the Committee of Ministers to consider the possibility of creating a European registry of national and international standards, with priority given to counterterrorism standards. To this effect, the CDCT has been publishing, since 2004, country-level briefs containing information on legislation and policies related to counterterrorism.

The CDCT cooperates closely with several international bodies, such as the Executive Directorate of the United Nations Counter-Terrorism Committee, the United Nations Office on Drugs and Crime, the Organization for Security and Cooperation in Europe, the European Union, and the Global Counter-Terrorism Forum. To efficiently counter terrorism, the Council of Europe has drawn up several conventions and protocols.

Among the most important conventions on terrorism are the European Convention for the Suppression of Terrorism, the European Convention for the Prevention of Terrorism, and the European Convention on Laundering, Investigation, Seizure and Confiscation of Crime-Related Returns.

The most important agreements related to other challenges that may lead to terrorism are the European Convention on Internet Crime, the Convention on Laundering, Searching for and Seizing Proceeds of Crime, the European Convention on Compensation for Victims of Violent Crimes, the European Convention on Transfer of Procedures in Criminal Matters, the European Convention on Mutual Assistance in Criminal Matters, and the European Convention of Extradition.

LONE WOLF TERRORISM

Dr. Mohd Yazid bin Zul Kepli

The term "lone wolves" refers to terrorists who commit acts of violence without coordination or affiliation with any groups. Unlike terrorist groups, lone wolves did not pose a major threat to the state, but now the situation has changed. COVID-19 pandemic has shown that a single individual can be a major threat to the state. It is recognized that individual terrorist attacks are less common vis-à-vis attacks by terrorist groups.

THREAT OF INDIVIDUAL ATTACKS

Individual attacks can be fatal. In 1995, American terrorist Timothy James McVeigh committed a massacre through bombing operations in Oklahoma City, killing 168 people and injured over 680 others. It is the deadliest terrorist attack in the USA history. In December of 2015, a couple attacked a birthday party in San Bernardino, which brought about the death of 14 people. In June of 2016, Omar Mateen killed 49 people at a nightclub in Orlando, Florida, in one of the most violent attacks on the USA soil since the 9/11 Attacks, 2001.

The concept of "lone wolves" dates back to 1983, when Lewis Beam, a member of the extremist Ku Klux Klan, and Arian Nations published a statement calling for "Resistance Without Leadership" toward the US government. Beam noted that intelligence agencies and law enforcement tools are not so effective against a reclusive individual who does not share his plans and intentions with others.

Since the mid-1990s, the number of terrorist crimes committed by "leaderless" rightwing extremists increased, leading up to the proliferation of lone wolf operations. On September 11, 2001, the terrorist attacks of Al-Qaeda resulted in horrific destruction and claimed many lives, which diverted attention from the rightwing extremists. The bombings in Bali, Istanbul and Mombasa and the train attacks in Madrid have been attributed to the emergence of Al-Qaeda terrorism.

IMPACT OF TERRORIST GROUPS

After Al-Qaeda, ISIS gained global notoriety in 2014, when it took control of Mosul and northern Iraq. By March 2019, however, ISIS had lost most of its territory in Iraq and Syria and was reduced down and whittled away into insurgent cells. Terrorist groups have learned from their losses in direct wars in the Middle East, and have followed various policies that feed on intensive propaganda on the internet and communication sites, by presenting emotionally loaded speeches and marking in bold relief what they consider corruption rife in governments.

Terrorist groups share their technical expertise, including making explosive devices using materials made available to all, while spreading methods for carrying out individual terrorist attacks on the internet. When sympathizers decide to act individually as lone wolves, they transform from mere sympathizers to active and dangerous terrorists.

SPECIFICITY OF LONE WOLVES

Lone wolves threaten their specificity, since when terrorists operate within a group, security services usually infiltrate the group, and law enforcement agencies and counterterrorism units can often track down group members. If any member is captured, the information gathered about the member captured would be very useful in determining the leadership structure and modus operandi of the group. This will eventually lead to the capture of the rest.

However, the situation becomes more complicated for lone wolves, as they can be very difficult to detect. This is especially so when they work on their own without contact or interaction, and they do not arouse suspicion, especially when they use light weapons such as knives, even when they use firearms, which are difficult to detect before the implementation of the terrorist operation.

Although lone wolves launch their attacks on their own, they often have some links with terrorist groups, such as communicating via the internet forums or social media. The radicalization of many lone wolves begins via the internet and the media. In 2013, researchers at Pennsylvania State University conducted a survey on the interaction of 119 lone wolf terrorists from different ideological, religious and cultural backgrounds. The findings revealed that 64% of the cases were friends and family members aware of the individual's intent to engage in terrorist activity.

Lone wolves can be a serious threat if they use a biological or viral weapon. In April 2020, two people in America were accused of committing terrorist crimes after they claimed that they were deliberately trying to spread COVID-19 virus. For the first case, the culprit was charged with perpetrating a biological weapons hoax and faces a maximum sentence of five years in federal prison. For the second case, the threat was found to be false.

PREVENTING LONE WOLVES

To prevent lone wolf attacks, various preventive steps can be taken. It is critically important to identify and address the root causes of terrorism. The Security Council Resolution 2250 issued in 2015 emphasizes the importance of addressing the conditions and factors that lead to extremism among youth. To this end, collective action and serious participation between communities and individuals in countering terrorism should be prioritized. Efforts to combat extremism should be organized and their impact measured accurately, and the use of soft and hard means should be in accordance with the requirements of the situation. De-radicalization efforts are sometimes more feasible, depending on the level of suspects' involvement. To this end, law enforcement authorities should first identify such suspects. The results of investigation and prosecution have proven repeatedly that when information becomes available and analyzed carefully, strategies and laws are more effective and successful.

The legal and institutional framework necessary should be put in place. This includes updated anti-money laundering and counter-financing of terrorism laws and effective coordination between local and international agencies. With the collective efforts of all parties, it is possible to prevent or at least reduce lone wolf attacks.

It should also be noted that COVID-19 pandemic has introduced new dimension to counterterrorism. COVID-19 pandemic is designated as a "biological agent" in certain countries like the USA. Therefore, those who threaten to spread it can be charged with terrorism. Other countries should equally follow suit. In addition, it is essential for all governments to cooperate and formulate a new policy in countering lone wolf terrorism especially in the context of biological weapon.

FUNNELING TERRORIST FINANCING THROUGH MONEY LAUNDERING

Dr. Emad Eddin Ahmed

Given the flagrant threat and destructive impact on the global economy along with the financial system and investment as well as the depletion of resources, money laundering and terrorist financing crimes have terrifyingly become the primary concern for the entire world. With this in mind, the international laws have unanimously criminalized such acts, and international organizations have rolled their sleeves to counter terrorist financing.

TERMINOLOGICAL DEFINITIONS

'Money laundering' means operations in which illicit funds are hidden to conceal the link with associated criminal activities in such a clandestine manner as to make the said money seem apparently legitimate with no cloud of suspicion lingering around. Against a backdrop of concealment, money laundering per se becomes easier to funnel the necessary resources for terrorist groups and organized gangs to carry out their activities that undermine global peace and security and whittle away at national and global economies. Equally important, inasmuch as financial systems are vulnerable and not resilient enough to accommodate the regional and continental differences of laws and regulations each country adopts, money laundering actors feed and capitalize on the fragile laws of anti-money laundering practices, especially in areas with legal controls that are much less sophisticated and are thus notoriously used by terrorists for their suspicious transactions.

Terrorist financing is associated with financial support for armed terrorist groups and organized crimes. Such practices are perpetrated by pooling legal or illegal funds, facilitating suspicious financial transactions, and supplying terrorists with funds around the world to launch their attacks on their set targets. Terrorist groups and criminal organizations need huge financial resources to aid and assist in carrying out their terrorist and criminal operations; they spare no efforts in collecting such dirty money to preserve their survival.

The American International Policy Center (2020) reveals that ISIS uses such funds to pay the salaries of staff and thus to ensure its survival, emphasizing that these funds greatly aid ISIS in maintaining its relationship with affiliated sleeper cells in Iraq, allocating $200 to $250 per soldier and $500 to $600 per commander per month. The Daily Telegraph published in an investigative report (2019) reveals that the British authorities discovered that billions of sterling pounds of British taxpayers' money were misappropriated and funneled through a secret network made up of British Asians, which was using clandestine routes across Pakistan and Afghanistan to transfer such funds to terrorist groups.

RESOURCES AND METHODS

The illegal financial resources made available for criminal activities are numerous, the most notorious of which are drug trafficking and contraband, illegal oil sale, human trafficking, antiquities theft, smuggling and selling arms, burglary, robbery, marauding plundering, blackmailing, looting, corruption and embezzlement, selling and buying currencies, along with illegal and suspicious financial transactions, using various methods through three key stages:

- **DEPOSIT:** It is the first stage and consists of depositing money and others in the financial system through international banks, commercial banks, postal banks, security companies, exchange offices, housing associations or any projects that can accept cash payment.

● **CONCEALMENT:** it is exchange of suspicious money and others with other assets, or transferring such money in a covert manner that cannot be tracked down by authorities. This includes trading in currencies, rapid investment in stocks and bonds, investing in insurance-based products, investing in joint ventures, or funneling money from one country to another, especially across fragile financial and legal procedures, such as Iran, Panama, the Bahamas and Mauritius.

● **CONSOLIDATION:** It is the final stage, which is the process of transferring suspicious funds allotted for illegal activity into legitimate assets and clean money, such as real estate, property, stocks, and cryptocurrencies (bitcoin).

These methods are not always sequential steps in criminal money laundering operations; such funds may be used directly in criminal or investment activity.

INTERNATIONAL EFFORTS

It is always critically necessary to tighten laws combating money laundering and terrorist financing across all countries of the world and to put into action joint international cooperation in addressing deadly epidemic, especially in the areas where terrorists take safe havens for their suspicious operations. Equally important, it is of great importance to constantly update these financial and legal laws and strengthen governance, financial management, integrity and safety locally, regionally and globally. This helps to bridge the gaps that terrorists and those complicit in money laundering can run through. The following international organizations and institutions are most active in combating money laundering:

Financial Action Task Force on Anti-Money Laundering (FATF)

The Financial Action Task Force (FATF) on anti-money laundering was established with the support of the G7 Summit in Paris in 1989; it includes 39 member countries, including the Kingdom of Saudi Arabia. FATF is mandated and entrusted with setting global standards for combating money laundering and terrorist financing in close cooperation with concerned international organizations, such as the World Bank, the International Monetary Fund (IMF), the United Nations (UN), the European Central Bank, and Interpol. FATF issues globally applicable recommendations and standards for national governments to better help in combating money laundering and terrorist financing. FATF has now more than 200 member countries and judicial authorities.

FATF has developed 40 recommendations on combating money laundering and nine recommendations on terrorist financing and criminalization of terrorism. The said recommendations include policies to combat money laundering and terrorist financing and coordination, financial sanctions related to such crimes, preventive measures for financial institutions, financial services and beneficiary transactions, high-risk countries, non-financial business and professions, transparency and ownership, financial intelligence units, responsibilities of law enforcement and investigation authorities, international cooperation measures, mutual legal aid, extradition treaties, and other systems, laws, legislations and procedures seeking to eliminate the two crimes of money laundering and terrorist financing.

Law Enforcement and Combating Organized Crime and Money Laundering Unit

The unit has been established within the United Nations Office on Drugs and Crime (UNODC) to implement the Global Program for Combating Money Laundering, Proceeds of Crime, and Financing of Terrorism launched in 1997 in response to the mandate, which the United Nations Office on Drugs and Crime was tasked with, according to the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, adopted in 1988. The responsibilities of the unit were further reinforced in 1998 with the political declaration and the adoption of anti-money laundering measures by the United Nations General Assembly at its twentieth special session.

International Monetary Fund

IMF made a significant contribution to combating money laundering and terrorist financing, through the Financial Sector Assessment Program and the External Financial Center Initiative, which included a full assessment of combating money laundering and terrorist financing. IMF launched a trust fund in 2009 to finance technical assistance in combating money laundering and terrorist financing, and Saudi Arabia well contributed to the said trust fund.

World Bank

In its financial operations, the World Bank encourages to take measures to combat the flow of illicit funds into the financial systems of the countries of the world to observe and notify the measures taken to combat money laundering and funneling terrorist financing.

MONEY LAUNDERING AND TECHNOLOGY

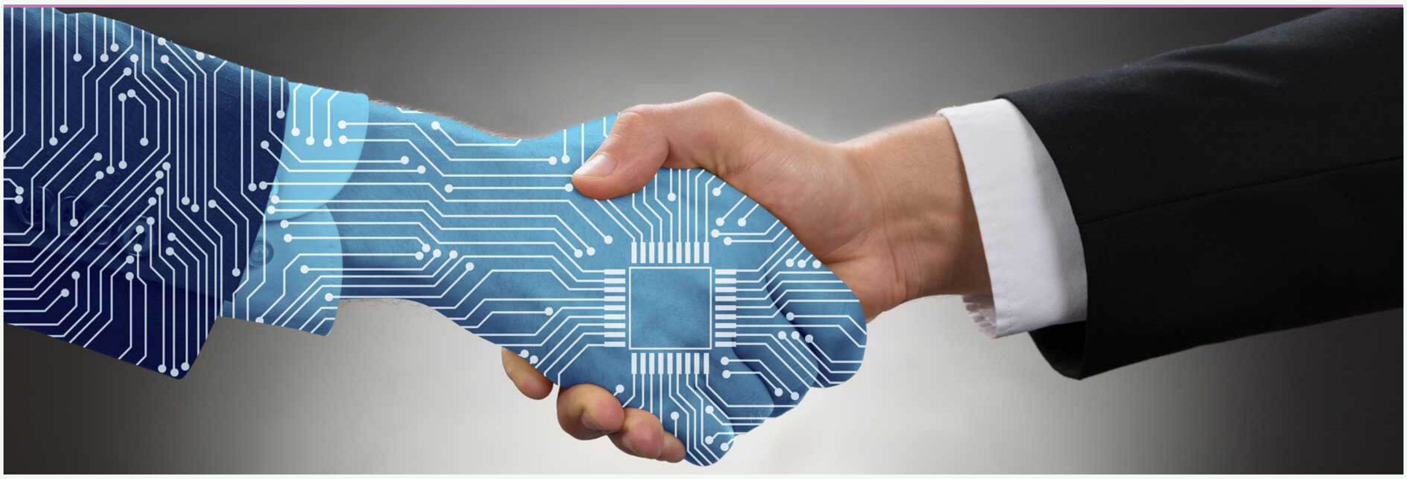
The rapid growth of encrypted assets, the sharp volatility in their exchange rates, and their ill-defined links with the traditional financial world could create new risk areas. In this regard, a report by the Spanish security services published in 2019 revealed that Fares Qatini, in charge of a terrorist cell affiliated with Al-Qaeda in Spain, was running a vast money-laundering network in Madrid and surrounding environs along with some eastern coastal cities in Spain, such as Castellón and Valencia. Qatini oversaw nine construction, transportation, health services, and elderly care companies, which he used to send money to Syria through the 'hawala' money transfer system used by Al-Qaeda to finance its activities and operations, through Turkey, Jordan, Lebanon and Syria.

Terrorist and criminal groups are always bypassing regulations to launder such money pooled from their criminal operations, most notorious are technology and the internet, especially the "deep web" and the "dark web" which have become a haven for terrorists. Therefore, countries and international organizations to combat money laundering and terrorist financing have attached great importance to such paramount issues, and sought to close the outlets that terrorists conduct in their business and trade. In 2017, the AlphaBay market, which was the largest market for online illicit transactions (drug trafficking, electronic piracy tools, weapons and toxic chemicals) for two years, was shut down, thankfully, following a large-scale operation spearheaded by the United States. Before closing the said market, more than a billion US dollars were traded using Bitcoin and other cryptocurrency assets. Bitcoin remains a hot-point of speculation, as it is not subject to any banking or legal supervision, and the circulation thereof is limited to electronic platforms.

RESEARCH CENTERS

GLOBAL NETWORK ON EXTREMISM AND TECHNOLOGY

ACADEMIC RESEARCH INITIATIVE FOR COUNTERTERRORISM AND DERADICALIZATION



With technology coming into play and mushrooming ubiquitously in various walks of life, extremists have sought to employ it to easily achieve their ends. This includes the use of the internet and social networking websites. They aim to sow and spread their extremist ideologies. With this in mind, it has become critically necessary to develop solutions and countermeasures against cyber-extremism, and the Global Network on Extremism and Technology (GNET) has just followed suit.

It is an independent academic research initiative supported by the Global Internet Forum on Counter-Terrorism (GIFCT), and funded by industrial enterprises, aimed at confronting terrorists, with a deeper understanding of their behavior and the methods of their use of technology. The GNET is overseen by the International Center for the Study of Radicalization (ICSR), a research center within the War Studies Department of King's College London.

The GNET leaders conduct research to find out more about the latest terrorist activities in the state-of-the-art technologies across America, Europe, Southeast Asia, and Australia, supported by a team deployed in North Africa, east of the Mediterranean Sea and South Asia.

The GNET enables experts to broadly investigate controversial issues related to extremist and technical-based violence; the GNET is based on solid research, high academic caliber and evidence to ensure actionable results. The GNET seeks to identify the relationship between the virtual and real activities of violent extremism, taking into account the human rights in freedom of expression and promoting academic cooperation among subject-matter researchers.

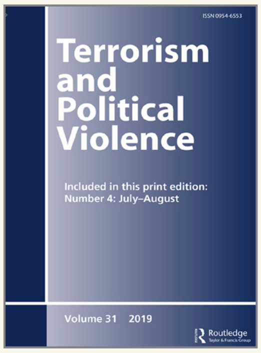
The GNET addresses six main research foci: the online-offline behavioral relationship and the associated evil, the balance between user privacy, state security and human rights, emerging or untimely patterns of violent extremism, improving academic cooperation between practitioners, sharing data and exchange of files and communication platforms, and exploring and explaining the limits of algorithmic measures.

The GNET realizes the importance of collecting terrorism-related information, scholars and analysts. It guarantees their freedom of action, and urges them to be fully aware of what they publish.

PERIODICALS

JOURNAL OF TERRORISM AND POLITICAL VIOLENCE

FOCUS OF ATTENTION OF RESEARCHERS AND DECISION-MAKERS



ISSN 0954-6553

Terrorism and Political Violence

Included in this print edition:
Number 4: July–August

Volume 31 2019

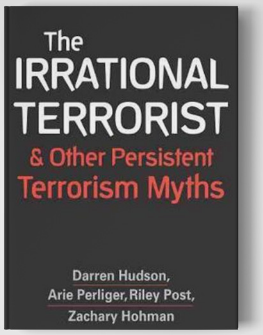
Routledge
Taylor & Francis Group

Link:

Terrorism and Political Violence is a multidisciplinary journal that promotes research related to political violence and terrorism, aimed at imparting academic robust engagement. The key foci include the links between political violence and organized crime, insurgent violence and states, demonstrations and acts of rebellion, revolutions, unrests, upheavals, riots, impact of social media, terrorism, human rights, terrorism and public policy, religion and violence, political parties and terrorism, technology and terrorism and far-right terrorism.

The Journal draws on a number of disciplines, theories and practical comparative approaches to present some leading actions in a segment that lacks precision. Special sections are designated for seminars and edited volumes for in-depth analyses of key issues. All research studies go through preliminary stages of examination, evaluation and peer-review. It has noticeably become a seminal nexus for decision-makers, subject-matter specialists and academics to further generate a better understanding of political violence.

THE IRRATIONAL TERRORIST AND OTHER PERSISTENT TERRORISM MYTHS



Author: Darren Hudson
Arie Perliger
Rile Post
Zachary Hohman
Publisher: Lynne Rienner Publishers
Date: January 28, 2020
ISBN-10: 1626378509

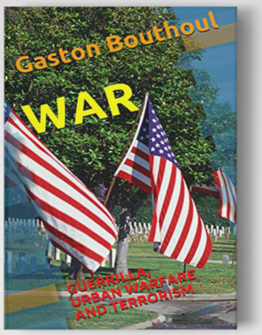
Link

Opinion surveys show that what the public assumes it knows about terrorism is a badly distorted view, being drummed up for. Although refuted by telling evidence, the ‘Flat Earth phenomenon made early misconceptions more solidified. The authors discredit such ubiquitous myths and misconceptions that feed on terrorism; they provide an easily accessible overview of the realities of terrorism and substantiate their analyses with case studies. They draw on the religious and economic backgrounds of terrorists to the nature and outreach of terrorist organizations. They also offer fact-based, cutting-edge explanations of the motivations and behavior of terrorist groups.

The said book addresses several topics relating to terrorism from various aspects: What We Think We Know About Terrorism; Myth: I Know Terrorism When I See It; Myth: Religious Fundamentalism Is the Only Source of Terrorism; Myth: Terrorists Are Poor and Uneducated; Myth: Terrorists Are Crazy; Myth: Terrorist Organizations Are Unsophisticated; The Influence of the Media and Governments; Four Critical Myths of Counterterrorism; Putting It All in Perspective.

First Myth: Terrorism (victims of despair); It is rumored that the terrorism that is sweeping our world is fueled by despair and loss of hope, and that we can change the situation by adopting a political process that gives terrorists some of what they aspire to, and claim that terrorism in this case will stop. Second Myth: terrorism (lone wolves). The media has adopted the idea that terrorism is ostensibly collective, but the execution of operations is triggered by individuals. Third Myth: (international support) to resolve the conflict. As this alleged support exists only within the limits of interests, without prejudice to the strength of the states’ relations with each other. There is another myth that has been addressed by the (RAND) study, according to which a person’s tendency to violence or terror can be predicted early, based on their origins or beliefs. This is an unfair, unjust and racist judgment that makes some beliefs extremist.

WAR: GUERRILLA, URBAN WARFARE AND TERRORISM



Author: Gaston Bouthoul
Publisher: The Author
Date: March 11, 2020
ASIN: B085THH654

Link

Polemology was first theorized, coined and posited by Gaston Bouthoul (1896 – 1980) as a stand-alone science. Later, polemology was put forward and addressed an interdisciplinary peace science, investigating the causes of wars, analyse their structure and consequences. Polemology aims to study dependent and independent premises of permanent peace to the national and international extent. The Second World War precipitated the realization of the said idea.

Bouthol (1945) founded Institut Français De Polémologie in Paris. To make it sound different among other terminologies, Bouthol termed it ‘polemology’ to be more precise and accurate in expressing the subject matter and individual characteristics towards the plans and methods related to warfare (strategies and tactics). According to the Greek source for the science of war, the subject-matter addresses warfare, belligerency, conflict, strife, combat and the laws governing warfare in different situations. Accordingly, this science aims at discovering the causes of wars and preserving people’s rights to life.

As for the cogency of the war scholars, it is to be aware of war to realize peace, which is embodied by the saying: "If you want peace, start studying war." This saying differs from the Roman saying: "If you want peace, prepare for war." There is a fundamental difference in the guidelines seeking peace.

Political scholars assume researching the phenomenon of war and armed conflict in a way that engages many disciplines, not just military disciplines. Knowledge of war fulfills important purposes for leading it efficiently. Military science (defense science) was intended to achieve victory over a potential adversary to secure sovereignty over the country. It is possible to benefit from the knowledge of war, its sources and causes in eliminating the phenomenon, and to initiate it at the same time as well. Therefore, the topic of war was both a science and an art within the area of interest of specialized researchers.

IMCTC MONTHLY SYMPOSIUM

UNDERSTANDING THE FORMS AND METHODS OF EXTREMISM AS A PRELUDE TO ADDRESSING IT BY MEDIA

IMCTC held a monthly symposium on 28/12/2020 in Riyadh, featuring "Understanding the Forms and Methods of Extremism as A Prelude to Addressing It by Media" presented by Dr. Fahd Abdul-Aziz Al-Ghofaili, in the presence of Major General Mohammed Saeed Al Moghedi, IMCTC Secretary-General, along with Lieutenant General (retd) Raheel Sharif, IMCTC Military Commander, delegates of the IMCTC member countries and IMCTC Center Personnel. Dr. Al-Ghofaili discussed the forms of extremism, tools and indicators of militant extremism, in addition to modern recruiting methods through media, digital platforms and methods of influence adopted by extremist terrorist groups.

Major General Al-Moghedi highlighted that the said symposium enhances counterterrorism through the media, as it reveals the methods and tools of extremist groups through digital and media platforms in recruitment.

STRATEGY HIGHLIGHTED IN WORKSHOPS CONDUCTED FOR IMCTC CENTER PERSONNEL

The IMCTC Center conducted training workshops for its personnel, themed "Strategy: General Concepts and Building Mechanisms" developed and presented by the IMCTC Center Strategy Department. The workshops addressed strategy concepts, objectives and characteristics, methods of developing a vision and mission, setting goals, and measuring key performance indicators (KPIs).

The said workshops were held for three days. Audio-visual presentations based on storytelling and narrative methods were utilized to communicate the concept of strategy and how to apply relevant tools and techniques in such a manner that ensures personnel's mastery of the implementation of strategic goals, while communicating operational and executive goals to their subordinates to achieve the goals of IMCTC. Several practical and hands-on exercises were provided in strategy building.