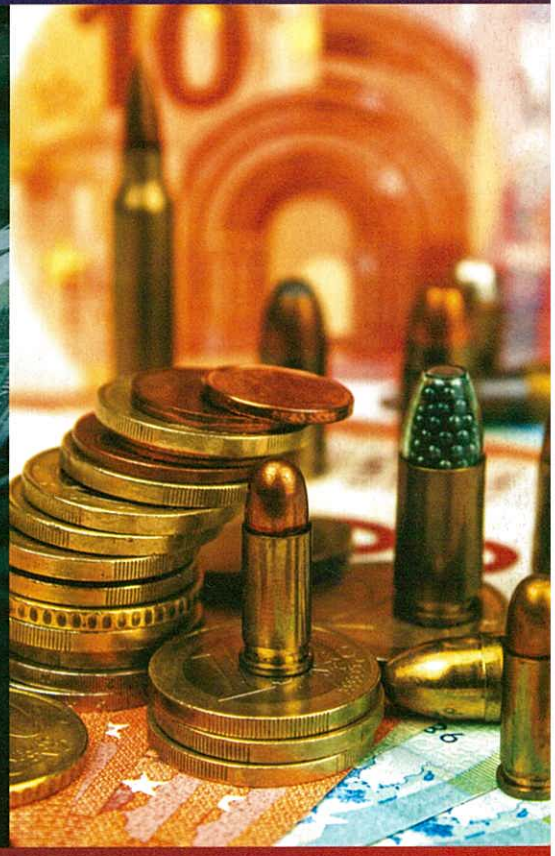
National Counter Terrorism Authority
(NACTA)

National Counter Terrorism Authority
(NACTA)



COVID-19
PANDEMIC

Money Laundering & Terrorist Financing Risks

National Counter Terrorism Authority (NACTA)

COVID-19 PANDEMIC

Money Laundering & Terrorist Financing (ML/TF) Risks

The COVID -19 pandemic has affected every stratum of society and is likely to reshape multiple dimensions of individual and public life. This unprecedented situation is likely to have considerable impact on the organized crime and terrorism landscape by exploiting the existing and emerging vulnerabilities. In this situation, the criminals may use their current modus operandi or resort to innovative criminal activities, especially when LEAs are engaged in COVID-19 related additional responsibilities. It is therefore imperative that the key ML/TF risk factors in COVID-19 scenario are given due attention and enhanced vigilance by LEAs, financial institutions and other relevant authorities is ensured.

National Counter Terrorism Authority (NACTA)

COVID-19 PANDEMIC

Do LEAs Know ML/TF Risks related to COVID-19 Crisis

Misuse of Charitable Sector:

- Possible attempts to exploit the pandemic funds
- Possible activity by UN listed/ proscribed organizations and any use of COVID-19 crisis to sneak back into raising money or engaging in social service activities
- Misuse of NPOs by unscrupulous elements

Cybercrime/Social Media:

- Use of COVID-19 crisis to carry out social engineering attacks
- Phishing email & spam mobile messages campaigns
- Fraudulent websites/ malicious attachments to seek and exploit personal payment information
- Use of cyberspace for propagation of extremist ideology & crowd funding

Virtual Assets:

- Use of Virtual Currencies (VCs) to launder proceeds earned from selling fraudulent or counterfeit COVID-19 related medicine/ goods
- Use of virtual assets to move and conceal illicit funds

Financial Frauds:

- Increase in financial fraud and scams and the offer of fraudulent investments in Ponzi schemes
- Fund raising scams in the name of treating COVID-19 patients
- Fraudulent investment schemes due to disruption in economic/financial activities

National Counter Terrorism Authority (NACTA)

COVID-19 PANDEMIC

Banking & Other Financial Services:

- Bypassing Customer Due Diligence (CDD) measures by exploiting temporary challenges in internal controls caused by remote working situations, in order to conceal and launder funds
- Abuse of vulnerabilities and suspicious transactions/activity through financial institutions

Increased Physical Cash Transactions:

- Criminals and terrorists exploiting COVID-19 and associated economic downturn may move into new cash-intensive and high-liquidity lines of business, both for the laundering of proceeds as well as to fund their operations

Unregulated Financial Services:

- Possible setback to the formal financial system
- Increased use of unregulated financial sector
- Opportunities for criminals and terrorists to launder or move illicit funds
- Prolonged economic recession may encourage non-traditional or unlicensed lenders, which may include criminal groups

Recruitment by Criminal/Terrorist Organizations:

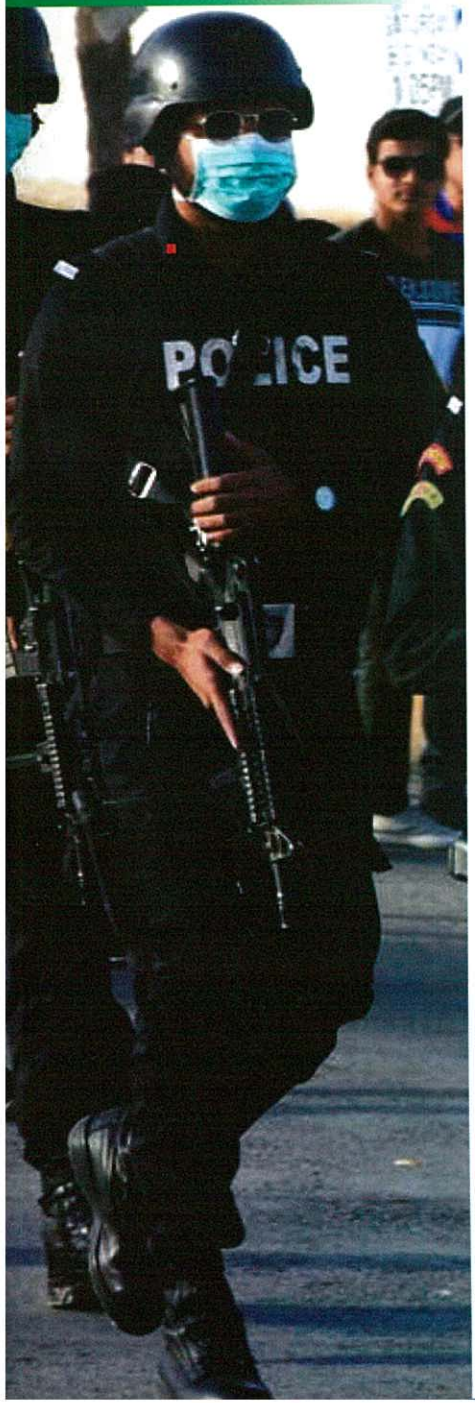
- Pandemic situation may lead to exploitation of vulnerable groups and criminal or terrorist organizations could exploit the situation for recruitment of people to support them in executing their activities

Narco-Trade/Trafficking:

- Possible increase in the drug use/business to overcome the depression/stress cause by the pandemic
- Criminals and terrorists may use drugs as a conduit for ML/TF

National Counter Terrorism Authority (NACTA)

COVID-19 PANDEMIC



LEAs as the Front Line of Defense

The risk and vulnerabilities posed by the current pandemic situation needs to be continuously and closely monitored for effective mitigation by:

- Enhancing LEAs' checks against misuse of charities/fund raising
- Not allowing UN listed/ proscribed entities and associated individuals to take any part in social welfare services
- Prioritizing investigation and prosecution of any COVID-19 related illicit ML/TF activity
- Keeping close watch on new typologies of misuse of COVID-19 situation for proactive response
- Communicating regularly with the private sector
- Monitoring very closely the cyber related frauds
- Countering extremism agenda via social media
- Encouraging reporting entities to remain vigilant and report suspicious transactions in case of any abuse of financial systems, particularly in the context of cross-border flows in relation to COVID-19 related funding