The Evolution of Global Organized Crime and Possible Future Trends

Global Initiative against Transnational Organized Crime
www.globalinitiative.net

Two Evolutionary Changes ('Mega-Trends') and Three Trends

- Spillover and diffusion of criminality
- Re-emergence of geopolitics
- Crime-terror convergence
- Fusing technology and physicality
- Crypto-crime and cyber-crime

Mega-Trend 1: Spillover and diffusion

Summary:
An increase in entrepreneurial crime, due to limited employment prospects for ‘globalized’ youth and ongoing transitions within established mafias

Mega-Trend 1: Spillover and diffusion

- Traditional mafia-style OC → penetration of state institutions and licit trans-border trade, flattening of hierarchies will ↑competition
  - ‘Kingpin strategy’ as template for leadership decapitation
  - Smaller, less centralized family units contributing to the weakeningof traditional (lineage-based) OC groups, allowing newer entrants into underworld with ethnically diverse networks
- ‘2008 generation’ of unemployed millennials is tech-savvy, educated manpower pool for smuggling syndicates
- Technical assistance improving trafficking (East European experts building narco-subs in Latin America, chemists disguising cocaine, former cigarette workers manufacturing fakes in EU)

Mega-Trend 1: Spillover and diffusion (Contd)

- States are not impervious to regional illicit trade (eg. AfPak heroin in Southern Africa, cocaine and politics in Antwerp)
- Brexit will reconfigure OC: ↑ in human trafficking and smuggling. Worst-case scenario: open border outside customs union (contraband movement more rewarding but not more risky)
- Limited fulltime employment for immigrants (legal & illegal) in EU, plus cultural clashes over values/norms, will fuel rise of street gangs who are already displacing ‘old’ mafias

Mega-Trend 2: Re-emergence of geopolitics

Summary:
Increasing international rivalries will shift international politics in favour of illicit trade in **some** sectors

Mega-Trend 2: Re-emergence of geopolitics

• States likely to use OC groups to covertly undermine each other (similar to 'deniable' patronage which sovereigns gave maritime piracy in centuries past):

- Sanctions-busting in East and West Asia : some governments investing in sophisticated counterfeiting infrastructure to forge US and Middle Eastern currency, using 'front companies' to acquire technology and material from the West

- Economic warfare: states using currency counterfeiting to create inflationary pressures in rivals and underwrite terrorist networks on a 'deniable' basis

• Speculation that governments may use OC actors for irredentist foreign policies, creating 'humanitarian crises' to justify military intervention

• OBOR (60 countries, 3 continents): will ↑trafficking in humans, drugs, wildlife, timber and maritime piracy due to high cargo flows (according to UNODC)

Trend 1: Crime-terror convergence

Summary:

Convergence is multi-faceted and features growing militarization of smaller-scale, local criminal entities

Trend 1: Crime-terror convergence

- Human, weapon smuggling are 2 key issues of C-T convergence
- Agrarian distress in traditional farming communities led to micro-economies of human smuggling, sustained by hearsay
- ↑arrivals in EU via Spain and Sicily (also, Black Sea). High risk of crossings could ↓family migration, but ↑youth radicalism
- 'Arms race' between gangs in EU as FF returnees/radicalized criminals seek illicit firearms for personal or political reasons

Trend 1: Crime-terror convergence (contd)

- Emerging OC groups prefer political instability, to use as cover for encroaching on turf of established OC groups
- Of US$31.5bn annually generated in conflict zones worldwide, 4% goes to ISIS. Most of remainder goes to OC groups
- Environmental crime is new money-spinner of terror (38% of worldwide insurgent finances, drugs = 28%, looting and extortion = 26%)
- Taliban diversified from narco-taxation to gem-smuggling, Al Shabaab earns revenue from charcoal and sugar rackets, ISIS steals antiques

Trend 2: Fusing technology with physicality

Summary:

Technology will not create new types of crime, but will enable existing crime to operate in new regions and in new ways

Trend 2: Fusing technology with physicality

- Interface of techno-crime and physical crime:

-Hackers track legitimate shipments contaminated with contraband, upon arrival gunmen seize containers in transit.

-Possessors of large cryptocurrency accounts mugged at knifepoint

- Smuggling via drones (East Europe – Lithuania, Ukraine, and East Asia – HK/China). Also possibly for assassination – Mexico.
- Expansion of mobile and data services (esp. WApp) facilitates *ad hoc* ('Uber-style') criminality – spot recruitment of mules to carry contraband for a flat fee
- Kimberley Process struggling to cope with new-generation smugglers, who mix conflict diamonds with certified ones
- Coded social media advertizing: sales of cheap-white cigarettes on FB through posting images with brand logos (FB does not allow open sales)

Trend 3: Crypto-crime and cyber-crime

Summary:

New technologies open up possibilities for both criminals and law enforcement, but the greater ease of operating them will pose a challenge to police in developing countries, who will need technical support from the West

Trend 3: Crypto-crime and cyber-crime

- Criminals presently favouring Ethereum, ZCash and Moreno over bitcoin (due to anonymity and transaction fees)
- 10% of investment in Ethereum-based ICOs in first nine months of 2017 went to criminals, due to weaknesses in blockchain coding
- 2018 study: 5x↑ in illegal activities using bitcoin (2013-16). 95% of laundered coins came from 9 DWmarkets (eg. Silk Road 1 and 2.0), 16% of coins were ransoms from malware attacks
- January 2018: US$523mn NEM coins stolen, half recovered/blocked
- Sanctioned states interested in creating national cryptocurrencies to assert autonomy (Venezuela – El Petro in January 2018)

Trend 3: Crypto-crime and cyber-crime (Contd)

- Some developing countries are becoming child-porn live-stream hubs, as mobile phones enable monetization of family and neighbourhood-level abuses
- Signs of slow-down in ransomware, due to availability of other means to monetize device capture (Cryptojacking uses bandwidth and processing power to mine e-currency without user's knowledge)
- WannaCry and NotPetya coopted system vulnerabilities such that their initiation did not depend on end-user compliance
- Forecast: there could be 146bn data breaches in 2018-23, with annual growth rate of 22.5%
- Healthcare records favourite target due to personal details, medical history and financial information

Thank you!

Prem Mahadevan
Global Initiative against Transnational Organized Crime
prem.mahadevan@globalinitiative.net